Introduzione.....2
Policy Argo del 14/04/2021.....3
Policy Argo del 15/03/2021.....11
Policy Argo del 22/12/2020.....20
Policy Argo del 30/06/2020.....28
Policy Argo del 05/04/2020.....36
Policy Argo del 20/01/2020.....43

Introduzione

In applicazione dei requisiti di trasparenza e per dare evidenza di tutte le modifiche effettuate sui servizi Argo, a livello di sicurezza delle informazioni, questo documento è reso disponibile a tutti i clienti nella sezione "Centro Notifiche" del Portale Argo, all'interno della scheda "Normativa" (https://www.portaleargo.it/argoweb/Notifiche.seam#).

Nel prosieguo sono quindi elencate tutte le Policy Web emesse e pubblicate sul sito della Argo nella pagina https://www.argosoft.it/privacy.php a far data dal 25 novembre 2019, che riepilogano le misure tecnologiche ed organizzative messe in atto dalla Argo ed accettate, con il contratto, dai clienti, per garantire la sicurezza delle informazioni ed il rispetto della normativa in materia di protezione dei dati personali.

In particolare in ogni documento sono:
- evidenziate in verde le parti aggiunte e migliorative delle garanzie offerte;
- barrate le parti eliminate;
- evidenziate in giallo le parti sostitutive di parti eliminate.

Policy Argo del 14/04/2021

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.
La Argo Software è impegnata costantemente nel migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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, Argo Software 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.
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.
Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software , nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, assistenza e manutenzione di software gestionale per le scuole di ogni ordine e grado e privati e di erogazione di servizi in modalità Cloud SaaS di gestione di documenti digitali anche a fini di conservazione, è inoltre certificato secondo la norma UNI CEI EN ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.] e sono adottati i controlli previsti dalle linee guida ISO/IEC 27017:2014 e ISO/IEC 27018:2019.

Tipologia dei dati e delle informazioni gestiti dalla Argo Software

I dati gestiti dalla Argo Software consistono nelle informazioni (generiche e personali) contenute negli archivi delle scuole e dei clienti fruitori dei medesimi servizi e nei profili degli utenti fruitori dei servizi web Argo.
In riferimento alle informazioni contenute negli archivi, la natura dei dati varia in base alle caratteristiche del servizio attivato da ogni singola istituzione scolastica o cliente. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, anche dati appartenenti alle categorie particolari di cui agli artt. 9 e 10 del Regolamento UE 2016/679 [specificamente quelle riepilogate nelle schede allegate al D.M. 305/2006, recante iden-

tificazione degli ex dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione].
I dati sono conservati all'interno dei database degli applicativi secondo la logica di raccolta e standardizzazione del singolo software ed etichettati secondo la classificazione delle informazioni del sistema di gestione.
I documenti sono raccolti e archiviati in appositi repository, secondo la logica di classificazione delle informazioni impostata dal cliente.

Modello di responsabilità condivisa (shared responsibility)

Argo Software 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 (anche di conservazione) 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 del servizio cloud, la Argo ha elaborato un documento che rappresenta il modello di responsabilità condivisa, disponibile alla pagina https://www.argosoft.it/privacy.php

Architettura del sistema informatico

I database server, i repository di documenti e le relative 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.
I database sono conservati nel servizio Amazon Aurora.
I file dei documenti sono conservati negli storage (contenitori) di Amazon S3.
I backup di database e file sono conservati negli storage di Amazon S3.
Per i dati dei propri clienti, Argo Software ha scelto la regione Europa Irlanda, situata nella Repubblica d'Irlanda, composta da 3 zone di disponibilità.
La Argo si avvale inoltre della Region Milano di Cloud AWS per i servizi di gestione di posta elettronica interni al software Argo Gecodoc.
L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative adottando il meccanismo di autenticazione forte a due fattori secondo un approccio basato sull'analisi dei rischi.

Con periodicità infrannuale, sulla base del piano degli audit interni, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato (auditor incaricato, DPO o responsabile del SGSI).
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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia, mediante l' Advanced Encryption Standard AES-256.
Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo 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 eseguita automaticamente la commutazione su una replica.

Backup e ripristino dei dati, garanzie di continuità operativa

Per ogni istanza di database, il servizio Amazon RDS esegue uno snapshot giornaliero e conserva i log delle modifiche al database all'interno del periodo di "retention" che segue**.** 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.
I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.
Per ciascuna istanza di database viene mantenuta una copia di backup giornaliera per 35 giorni (periodo di retention dei backup).
Settimanalmente (domenica), è inoltre effettuata una ulteriore copia di tutti i dati.
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 per ulteriori 25 giorni.
Per offrire un pari livello di protezione anche ai documenti, la Argo ha attivato la funzione *Versioning* che consente di recuperare e ripristinare qualsiasi versione di ogni file di documento memorizzato nello storage Amazon S3.
Il servizio di AWS garantisce una durabilità dei dati pari ad oltre il 99,9% perchè crea e mantiene automaticamente copie di tutti gli oggetti su più sistemi.
Per tutelare i propri clienti, la Argo ha messo in funzione un piano di continuità operativa molto dettagliato, che mira a garantire il ripristino di tutte le informazioni contenute nelle repliche anche in caso di disastro, secondo i seguenti SLA:
RTO: il tempo massimo di recupero e ripristino delle informazioni è fissato in 4 ore dall’incidente.
RPO: il punto massimo di perdita di dati in caso di incidente è 24 ore (per via del backup giornaliero, se l’incidente avviene prima della copia, il massimo di dati persi è fino all’ultima esecuzione del backup del giorno precedente).

I due SLA, combinati, mirano a garantire ai clienti dei servizi cloud che in caso di disastro, la Argo sarà in grado di ripristinare la disponibilità di tutti i dati, fatti salvi quelli registrati nelle ultime 24 ore, in un massimo di 4 ore.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.
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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.
L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Utilizzo delle utenze Argo per accesso ad altri servizi

Attraverso l'utenza Argo docente o genitore o alunno è possibile accedere ai servizi di e-learning offerti da BSMART.
L'autenticazione avviene utilizzando il protocollo di sicurezza OAuth2, il quale permette di accedere ai servizi forniti da applicazioni terze senza fornire a quest'ultime le credenziali di accesso (sulle quali quindi l'utente e Argo continuano ad avere esclusivo controllo).
L'accesso ai servizi BSMART utilizzando le credenziali Argo è naturalmente facoltativo e in caso di accettazione da parte dell'utente, l'utente è reindirizzato dalla piattaforma BSMART ad un dominio Argo, unico punto di accesso da cui viene consentito trasmettere le proprie credenziali Argo.
Al termine del processo di autenticazione, l'utente viene rimandato sul dominio del *client* da cui ha avuto origine la richiesta, e precedentemente autorizzato dalla Argo.
I dati forniti a BSMART si riferiscono esclusivamente a nome, cognome, codice fiscale, indirizzo email, ruolo (docente, genitore o alunno).
Le attività svolte da BSMART nell’erogazione dei servizi di e-learning, anche se accedute con credenziali Argo, sono agite in assoluta autonomia e sotto la responsabilità di BSMART che agisce in qualità di titolare del trattamento.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo e – per le applicazioni più critiche - delle operazioni effettuate dagli utenti all'interno degli stessi. I dati relativi agli accessi ed alle operazioni sono conservati per un periodo di 24 mesi. Per le eventuali richieste dei Log da parte dei clienti, l'Azienda richiede la compilazione di apposita modulista da inviare tramite PEC all'indirizzo assistenza.argo@pec.ecert.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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.
Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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/IEC 27001, la qualificazione come CSP presso AgID, uno SLA di connettività di almeno il 95% su base annua ed una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

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

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.
Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, 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 ed i documenti 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, più i tempi di retention del backup sopra indicati (35+25 gg = 2 mesi), a seconda della natura delle informazioni 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.
Il tempo massimo di conservazione dei dati contenuti nei database dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi.
Parimenti, il tempo massimo di conservazione dei documenti contenuti nei repository dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi, al termine dei quali la Argo procederà alla cancellazione logica dei files dai sistemi. L'attivazione del versioning nei repository richiede però anche una operazione di cancellazione fisica (manuale) da parte degli amministratori di sistema, che sarà effettuata con frequenza almeno annuale per tutti i contratti cessati. Di conseguenza, la Argo potrà conservare fisicamente i documenti caricati nelle applicazioni per un ulteriore periodo di massimo 12 mesi.

Impegni e garanzie per la protezione dei dati personali

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.
Per la fornitura dei servizi web, la Argo Software 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://assistenza.argo.software/utilities/.
In caso di assenza di nomina formale, la Argo Software 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 Argo Software, è Chiara Delaini, raggiungibile all'indirizzo di posta elettronica ordinario dpo@argosoft.it o di posta elettronica certificata dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte dei clienti o degli interessati.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software s.r.l. assume in sintesi 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 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 diverse 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 violazione di dati personali ai fini della registrazione/notifica/comunicazione dei data breach;
- provvedere immediatamente, nel caso in cui un interessato si rivolgesse alla Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Valutazione dei rischi per la sicurezza delle informazioni

La Argo Software mantiene aggiornate le proprie valutazioni dei rischi per la sicurezza delle informazioni e per la protezione dei dati personali, secondo quanto previsto dal Sistema di Gestione per la Sicurezza delle Informazioni certificato.
Agendo in qualità di Responsabile del Trattamento, la Argo non ha proceduto ad effettuare alcuna valutazione di impatto ai sensi dell'articolo 25 del GDPR, ma collabora (tramite gli esiti delle valutazioni dei rischi di cui sopra) con i Titolari del Trattamento che decidessero di effettuare DPIA su trattamenti effettuati anche tramite gli applicativi web Argo.
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 della Argo Software.

Comunicazione di eventuali incidenti o potenziali violazioni

Qualunque incidente o potenziale incidente occorso tramite o durante l'utilizzo di un applicativo Argo, che contempli o meno la presenza di dati personali, deve essere immediatamente comunicato dalla scuola agli appositi canali di assistenza Argo (telefono, e-mail, o ArgoHelp).
Il servizio assistenza Argo 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.
All'apertura effettiva di un incidente, terminata la verifica preliminare, il servizio assistenza segue la procedura interna per la gestione degli incidenti e la documenta secondo quanto previsto dal Sistema di Gestione per le Informazioni.
Nel caso in cui l'incidente, accertato, riguardasse anche dati personali, l'Ufficio Privacy della Argo effettua tutti i passaggi, sostanziali e formali, per la verifica della sussitenza, 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, l'Ufficio Privacy documenta opportunamente il data breach nel Registro degli Incidenti Argo e procede alla comunicazione dello stesso al Titolare del Trattamento nel tempo massimo di 48 ore dalla avvenuta conoscenza ed analisi dell'incidente.
In dipendenza del tipo e della gravità dell'incidente occorso, quindi, l'Ufficio Privacy Argo 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 Argo e la eventuale comunicazione ad altri soggetti (Titolari o Responsabili del Trattamento) coinvolti nell'incidente.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale Argo.

Ultimo aggiornamento 14/04/2021

Policy Argo del 15/03/2021

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.

La Argo Software è impegnata costantemente nel migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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, Argo Software 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.
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.

Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software , nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, assistenza e manutenzione di software gestionale per le scuole di ogni ordine e grado e privati e di erogazione di servizi in modalità Cloud SaaS di gestione di documenti digitali anche a fini di conservazione, è inoltre certificato secondo lo standard ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.] e sono adottati i controlli previsti dalle linee guida ISO /IEC 27017:2015 e ISO/IEC 27018:2019

Tipologia dei dati e delle informazioni gestiti dalla Argo Software

I dati gestiti dalla Argo Software consistono nelle informazioni (generiche e personali) contenute negli archivi delle scuole e dei clienti fruitori dei medesimi servizi e nei profili degli utenti fruitori dei servizi web Argo.

In riferimento alle informazioni contenute negli archivi, la natura dei dati varia in base alle caratteristiche del servizio attivato da ogni singola istituzione scolastica o cliente. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, anche dati appartenenti alle categorie particolari di cui agli artt. 9 e 10 del Regolamento UE 2016/679 [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].

Modello di responsabilità condivisa (shared responsibility)

Argo Software 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 (anche di conservazione) 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 del servizio cloud, la Argo ha elaborato un documento che rappresenta il modello di responsabilità condivisa, disponibile alla pagina https://www.argosoft.it/privacy.php

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 dei propri clienti, Argo Software ha scelto la regione Europa Irlanda, situata nella Repubblica d'Irlanda, composta da 3 zone di disponibilità.

~~La Argo si avvale inoltre, come Cloud Service Provider qualificato, dei servizi di Aruba spa per la gestione di alcuni servizi accessori al sistema documentale.~~
La Argo si avvale inoltre della Region Milano di Cloud AWS per i servizi di gestione di posta elettronica interni al software Argo Gecodoc.

L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative.

Con periodicità infrannuale, sulla base del piano degli audit interni, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato (auditor incaricato, DPO o responsabile del SGSI).
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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia, mediante l' Advanced Encryption Standard AES-256.

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo 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 eseguita automaticamente la commutazione su una replica.

Backup e ripristino dei dati, garanzie di continuità operativa

Per ogni istanza di database, il servizio Amazon RDS esegue uno snapshot giornaliero e conserva i log delle modifiche al database all'interno del periodo di "retention" che segue. 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.
I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.

Per ciascuna istanza di database viene mantenuta una copia di backup giornaliera per 35 giorni (periodo di retention dei backup).
Settimanalmente (domenica), è inoltre effettuata una ulteriore copia di tutti i dati
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 per ulteriori 25 giorni.

Per tutelare i propri clienti, la Argo ha messo in funzione un piano di continuità operativa molto dettagliato, che mira a garantire il ripristino di tutte le informazioni contenute nelle repliche anche in caso di disastro, secondo i seguenti SLA:
RTO: il tempo massimo di recupero e ripristino delle informazioni è fissato in 4 ore dall'incidente
RPO: il punto massimo di perdita di dati in caso di incidente è 24 ore (per via del backup giornaliero, se l'incidente avviene prima della copia, il massimo di dati persi è fino all'ultima esecuzione del backup del giorno precedente).

I due SLA, combinati, mirano a garantire ai clienti dei servizi cloud che in caso di disastro, la Argo sarà in grado di ripristinare la disponibilità di tutti i dati, fatti salvi quelli registrati nelle ultime 24 ore, in un massimo di 4 ore.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.

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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Utilizzo delle utenze Argo per accesso ad altri servizi

Attraverso l'utenza Argo docente o genitore o alunno è possibile accedere ai servizi di e-learning offerti da BSMART.

L'autenticazione avviene utilizzando il protocollo di sicurezza OAuth2, il quale permette di accedere ai servizi forniti da applicazioni terze senza fornire a quest'ultime le credenziali di accesso (sulle quali quindi l'utente e Argo continuano ad avere esclusivo controllo).

L'accesso ai servizi BSMART utilizzando le credenziali Argo è naturalmente facoltativo e in caso di accettazione da parte dell'utente, l'utente è reindirizzato dalla piattaforma BSMART ad un dominio Argo, unico punto di accesso da cui viene consentito trasmettere le proprie credenziali Argo.

Al termine del processo di autenticazione, l'utente viene rimandato sul dominio del *client* da cui ha avuto origine la richiesta, e precedentemente autorizzato dalla Argo.

I dati forniti a BSMART si riferiscono esclusivamente a nome, cognome, codice fiscale, indirizzo email, ruolo (docente, genitore o alunno).

Le attività svolte da BSMART nell’erogazione dei servizi di e-learning, anche se accedute con credenziali Argo, sono agite in assoluta autonomia e sotto la responsabilità di BSMART che agisce in qualità di titolare del trattamento.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo e – per le applicazioni più critiche - delle operazioni effettuate dagli utenti all'interno degli stessi. I dati relativi agli accessi ed alle operazioni sono conservati per un periodo di 24 mesi. Per le eventuali richieste dei Log da parte dei clienti, l'Azienda richiede la compilazione di apposita modulista da inviare tramite PEC all'indirizzo assistenza.argo@pec.ecert.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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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 95% su base annua ed una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

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

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di

backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, 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, più i tempi di retention del backup sopra indicati (35+25 gg=2 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.

Il tempo massimo di conservazione dei dati dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi.

Impegni e garanzie per la protezione dei dati personali

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.
Per la fornitura dei servizi web, la Argo Software 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://assistenza.argo.software/utilities/.
In caso di assenza di nomina formale, la Argo Software 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 Argo Software, è Chiara Delaini, raggiungibile all'indirizzo di posta elettronica ordinario dpo@argosoft.it o di posta elettronica certificata dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte dei clienti o degli interessati.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software s.r.l. assume in sintesi 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 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 diverse 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 violazione di dati personali ai fini della registrazione/notifica/comunicazione dei data breach;
- provvedere immediatamente, nel caso in cui un interessato si rivolgesse alla Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Valutazione dei rischi per la sicurezza delle informazioni

La Argo Software mantiene aggiornate le proprie valutazioni dei rischi per la sicurezza delle informazioni e per la protezione dei dati personali, secondo quanto previsto dal Sistema di Gestione per la Sicurezza delle Informazioni certificato.
Agendo in qualità di Responsabile del Trattamento, la Argo non ha proceduto ad effettuare alcuna valutazione di impatto ai sensi dell'articolo 25 del GDPR, ma collabora (tramite gli esiti delle valutazioni dei rischi di cui sopra) con i Titolari del Trattamento che decidessero di effettuare DPIA su trattamenti effettuati anche tramite gli applicativi web Argo.
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 della Argo Software.

Comunicazione di eventuali incidenti o potenziali violazioni

Qualunque incidente o potenziale incidente occorso tramite o durante l'utilizzo di un applicativo Argo, che contempli o meno la presenza di dati personali, deve essere immediatamente comunicato dalla scuola agli appositi canali di assistenza Argo (telefono, e-mail, o ArgoHelp).
Il servizio assistenza Argo 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.
All'apertura effettiva di un incidente, terminata la verifica preliminare, il servizio assistenza segue la procedura interna per la gestione degli incidenti e la documenta secondo quanto previsto dal Sistema di Gestione per le Informazioni.
Nel caso in cui l'incidente, accertato, riguardasse anche dati personali, l'Ufficio Privacy della Argo effettua tutti i passaggi, sostanziali e formali, per la verifica della sussitenza, 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, l'Ufficio Privacy documenta opportunamente il data breach nel Registro degli Incidenti Argo e procede alla comunicazione dello stesso al Titolare del Trattamento nel tempo massimo di 48 ore dalla avvenuta conoscenza ed analisi dell'incidente.
In dipendenza del tipo e della gravità dell'incidente occorso, quindi, l'Ufficio Privacy Argo 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 Argo e la eventuale comunicazione ad altri soggetti (Titolari o Responsabili del Trattamento) coinvolti nell'incidente.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale Argo.

Ultimo aggiornamento 15/03/2021

Policy Argo del 22/12/2020

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.

La Argo Software è impegnata costantemente nel migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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, Argo Software 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.
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.

Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software , nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, assistenza e manutenzione di software gestionale per le scuole di ogni ordine e grado e privati e di erogazione di servizi in modalità Cloud SaaS di gestione di documenti digitali anche a fini di conservazione, è inoltre certificato secondo lo standard ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.] e sono adottati i controlli previsti dalle linee guida ISO /IEC 27017:2015 e ISO/IEC 27018:2019

Tipologia dei dati e delle informazioni gestiti dalla Argo Software

I dati gestiti dalla Argo Software consistono nelle informazioni (generiche e personali) contenute negli archivi delle scuole e dei clienti fruitori dei medesimi servizi e nei profili degli utenti fruitori dei servizi web Argo.

In riferimento alle informazioni contenute negli archivi, la natura dei dati varia in base alle caratteristiche del servizio attivato da ogni singola istituzione scolastica o cliente. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, anche dati appartenenti alle categorie particolari di cui agli artt. 9 e 10 del Regolamento UE 2016/679 [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].

Modello di responsabilità condivisa (shared responsibility)

Argo Software 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 (anche di conservazione) 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 del servizio cloud, la Argo ha elaborato un documento che rappresenta il modello di responsabilità condivisa, disponibile alla pagina https://www.argosoft.it/privacy.php

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 dei propri clienti, Argo Software ha scelto la regione Europa Irlanda, situata nella Repubblica d'Irlanda, composta da 3 zone di disponibilità.

La Argo si avvale inoltre, come Cloud Service Provider qualificato, dei servizi di Aruba spa per la gestione di alcuni servizi accessori al sistema documentale.

L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative.
Con periodicità infrannuale, sulla base del piano degli audit interni, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato (auditor incaricato, DPO o responsabile del SGSI).

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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia, mediante l' Advanced Encryption Standard AES-256.

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo 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 eseguita automaticamente la commutazione su una replica.

Backup dei dati

Per ogni istanza di database, il servizio Amazon RDS esegue uno snapshot giornaliero e conserva i log delle modifiche al database all'interno del periodo di "retention" che segue**.** 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.
I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.

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.
Decorso questo periodo, viene mantenuta una copia settimanale per ulteriori 25 giorni.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.

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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da

parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Utilizzo delle utenze Argo per accesso ad altri servizi

Attraverso l'utenza Argo docente o genitore o alunno è possibile accedere ai servizi di e-learning offerti da BSMART.

L'autenticazione avviene utilizzando il protocollo di sicurezza OAuth2, il quale permette di accedere ai servizi forniti da applicazioni terze senza fornire a quest'ultime le credenziali di accesso (sulle quali quindi l'utente e Argo continuano ad avere esclusivo controllo).

L'accesso ai servizi BSMART utilizzando le credenziali Argo è naturalmente facoltativo e in caso di accettazione da parte dell'utente, l'utente è reindirizzato dalla piattaforma BSMART ad un dominio Argo, unico punto di accesso da cui viene consentito trasmettere le proprie credenziali Argo.

Al termine del processo di autenticazione, l'utente viene rimandato sul dominio del *client* da cui ha avuto origine la richiesta, e precedentemente autorizzato dalla Argo.

I dati forniti a BSMART si riferiscono esclusivamente a nome, cognome, codice fiscale, indirizzo email, ruolo (docente, genitore o alunno).

Le attività svolte da BSMART nell'erogazione dei servizi di e-learning, anche se accedute con credenziali Argo, sono agite in assoluta autonomia e sotto la responsabilità di BSMART che agisce in qualità di titolare del trattamento.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo e – per le applicazioni più critiche - delle operazioni effettuate dagli utenti all'interno degli stessi. I dati relativi agli accessi ed alle operazioni sono conservati per un periodo di 24 mesi. Per le eventuali richieste dei Log da parte dei clienti, l'Azienda richiede la compilazione di apposita modulista da inviare tramite PEC all'indirizzo assistenza.argo@pec.ecert.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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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 95% su base annua ed una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

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

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, 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, più i tempi di retention del backup sopra indicati (35+25 gg=2 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.~~ Il tempo massimo di conservazione dei dati dopo la cessazione del contratto e/o la richiesta di cancellazione dei dati è 12+2 mesi.

Impegni e garanzie per la protezione dei dati personali

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.
Per la fornitura dei servizi web, la Argo Software 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://assistenza.argo.software/utilities/.
In caso di assenza di nomina formale, la Argo Software 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 Argo Software, è Chiara Delaini, raggiungibile all'indirizzo di posta elettronica ordinario dpo@argosoft.it o di posta elettronica certificata dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte dei clienti o degli interessati.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software s.r.l. assume in sintesi 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 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 diverse 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 violazione di dati personali ai fini della registrazione/notifica/comunicazione dei data breach;
- provvedere immediatamente, nel caso in cui un interessato si rivolgesse alla Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Valutazione dei rischi per la sicurezza delle informazioni

La Argo Software mantiene aggiornate le proprie valutazioni dei rischi per la sicurezza delle informazioni e per la protezione dei dati personali, secondo quanto previsto dal Sistema di Gestione per la Sicurezza delle Informazioni certificato.
Agendo in qualità di Responsabile del Trattamento, la Argo non ha proceduto ad effettuare alcuna valutazione di impatto ai sensi dell'articolo 25 del GDPR, ma collabora (tramite gli esiti delle valu-

tazioni dei rischi di cui sopra) con i Titolari del Trattamento che decidessero di effettuare DPIA su trattamenti effettuati anche tramite gli applicativi web Argo.
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 della Argo Software.

Comunicazione di eventuali incidenti o potenziali violazioni

Qualunque incidente o potenziale incidente occorso tramite o durante l'utilizzo di un applicativo Argo, che contempli o meno la presenza di dati personali, deve essere immediatamente comunicato dalla scuola agli appositi canali di assistenza Argo (telefono, e-mail, o ArgoHelp).
Il servizio assistenza Argo 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.
All'apertura effettiva di un incidente, terminata la verifica preliminare, il servizio assistenza segue la procedura interna per la gestione degli incidenti e la documenta secondo quanto previsto dal Sistema di Gestione per le Informazioni.
Nel caso in cui l'incidente, accertato, riguardasse anche dati personali, l'Ufficio Privacy della Argo effettua tutti i passaggi, sostanziali e formali, per la verifica della sussitenza, 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, l'Ufficio Privacy documenta opportunamente il data breach nel Registro degli Incidenti Argo e procede alla comunicazione dello stesso al Titolare del Trattamento nel tempo massimo di 48 ore dalla avvenuta conoscenza ed analisi dell'incidente.
In dipendenza del tipo e della gravità dell'incidente occorso, quindi, l'Ufficio Privacy Argo 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 Argo e la eventuale comunicazione ad altri soggetti (Titolari o Responsabili del Trattamento) coinvolti nell'incidente.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale Argo.

Ultimo aggiornamento 22/12/2020

Policy Argo del 30/06/2020

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.

La Argo Software è impegnata costantemente a migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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, Argo Software 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.
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.

Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software srl, nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, è inoltre certificato secondo lo standard ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.].

Tipologia dei dati e delle informazioni gestiti dalla Argo Software

I dati gestiti dalla Argo Software riguardano le informazioni (generiche e personali) contenute negli archivi delle scuole fruitrici dei medesimi servizi ed i profili degli utenti fruitori dei servizi web Argo.

In riferimento alle informazioni contenute negli archivi delle scuole, la natura dei dati varia in base alle caratteristiche del servizio attivato da ogni singola istituzione scolastica. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, anche dati appartenenti alle categorie particolari di cui all'art. 9 del Regolamento UE 2016/679 [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].

Modello di responsabilità condivisa (shared responsibility)

Argo Software 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 (anche di conservzione) 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 del servizio cloud, la Argo ha elaborato un documento che rappresenta il modello di responsabilità condivisa, disponibile alla pagina https://www.argosoft.it/privacy.php

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, proprie clienti, Argo Software 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 alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative.
Con periodicità infrannuale, sulla base del piano degli audit interni, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato (auditor incaricato, DPO o responsabile del SGSI).
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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia, mediante l' Advanced Encryption Standard AES-256.

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo, 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 eseguita automaticamente la commutazione su una replica.

Backup dei dati

Per ogni istanza di database, il servizio Amazon RDS 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.

I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.

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.
Decorso questo periodo, viene mantenuta una copia settimanale per ulteriori 25 giorni.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.

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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli

aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Utilizzo delle utenze Argo per accesso ad altri servizi

Attraverso l'utenza Argo docente o genitore o alunno è possibile accedere ai servizi di e-learning offerti da BSMART.
L'autenticazione avviene utilizzando il protocollo di sicurezza OAuth2, il quale permette di accedere ai servizi forniti da applicazioni terze senza fornire a quest'ultime le credenziali di accesso (sulle quali quindi l'utente e Argo continuano ad avere esclusivo controllo).

L'accesso ai servizi BSMART utilizzando le credenziali Argo è naturalmente facoltativo e in caso di accettazione da parte dell'utente, l'utente è reindirizzato dalla piattaforma BSMART ad un dominio Argo, unico punto di accesso da cui viene consentito trasmettere le proprie credenziali Argo.
Al termine del processo di autenticazione, l'utente viene rimandato sul dominio del *client* da cui ha avuto origine la richiesta, e precedentemente autorizzato dalla Argo.

I dati forniti a BSMART si riferiscono esclusivamente a nome, cognome, codice fiscale, indirizzo email, ruolo (docente, genitore o alunno).
Le attività svolte da BSMART nell'erogazione dei servizi di e-learning, anche se accedute con credenziali Argo, sono agite in assoluta autonomia e sotto la responsabilità di BSMART che agisce in qualità di titolare del trattamento.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo 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 le eventuali richieste dei Log da parte dei clienti, l'Azienda richiede la compilazione di apposita modulista da inviare tramite PEC all'indirizzo assistenza.argo@pec.ecert.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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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 95% su base annua ed una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

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

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, 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

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.

Per la fornitura dei servizi web, la Argo Software 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://www.portaleargo.it/docs/nomina.pdf.
In caso di assenza di nomina formale, la Argo Software 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 Argo Software, è Chiara Delaini, raggiungibile all'indirizzo dpo@argosoft.it o dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte della scuola.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software 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 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 diverse 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 Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Valutazione dei rischi per la sicurezza delle informazioni

La Argo Software mantiene aggiornate le proprie valutazioni dei rischi per la sicurezza delle informazioni e per la protezione dei dati personali, secondo quanto previsto dal Sistema di Gestione per la Sicurezza delle Informazioni certificato.
Agendo in qualità di Responsabile del Trattamento, la Argo non ha proceduto ad effettuare alcuna valutazione di impatto ai sensi dell'articolo 25 del GDPR, ma collabora (tramite gli esiti delle valutazioni dei rischi di cui sopra) con i Titolari del Trattamento che decidessero di effettuare DPIA su trattamenti effettuati anche tramite gli applicativi web Argo.

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 della Argo Software.

Comunicazione di eventuali incidenti o potenziali violazioni

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

Il servizio assistenza Argo 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.
All'apertura effettiva di un incidente, terminata la verifica preliminare, il servizio assistenza segue la procedura interna per la gestione degli incidenti e la documenta secondo quanto previsto dal Sistema di Gestione per le Informazioni.
Nel caso in cui l'incidente, accertato, riguardasse anche dati personali, l'Ufficio Privacy della Argo effettua tutti i passaggi, sostanziali e formali, per la verifica della sussitenza, 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, l'Ufficio Privacy documenta opportunamente il data breach nel Registro degli Incidenti Argo e procede alla comunicazione dello stesso al Titolare del Trattamento.
In dipendenza del tipo e della gravità dell'incidente occorso, quindi, l'Ufficio Privacy Argo 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 Argo e la eventuale comunicazione ad altri soggetti (Titolari o Responsabili del Trattamento) coinvolti nell'incidente.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale argo.

Ultimo aggiornamento 30/06/2020

Policy Argo del 05/04/2020

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza informatica, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.

La Argo software srl è impegnata costantemente a migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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.

Nell'ambito della continuità operativa, Argo Software adotta tutti gli accorgimenti organizzativi, le soluzioni tecniche e procedurali idonee al 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.).
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.

Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software srl, nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, è inoltre certificato secondo lo standard ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.].

Tipologia dei dati gestiti dalla Argo Software

I dati gestiti dalla Argo Software riguardano le informazioni (generiche e personali) contenute negli archivi delle scuole fruitrici dei medesimi servizi ed i profili degli utenti fruitori dei servizi web Argo.

In riferimento alle informazioni contenute negli archivi delle scuole, la natura dei dati varia in base alle caratteristiche del servizio attivato dalla scuola. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, possono essere trattati anche dati appartenenti alle categorie particolari di cui all'art. 9 del Regolamento UE 2016/679 [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 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, proprie clienti, Argo Software 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 alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative.
Con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del personale all'uopo 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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia*, mediante l' Advanced Encryption Standard AES-256.*

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo, 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, il servizio Amazon RDS 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.
I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.

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.
Decorso questo periodo, viene mantenuta una copia settimanale per ulteriori 25 giorni.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.

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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Utilizzo delle utenze Argo per accesso ad altri servizi.

Attraverso l'utenza Argo docente o genitore o alunno è possibile accedere ai servizi di e-learning offerti da BSMART.
L'autenticazione avviene utilizzando il protocollo di sicurezza OAuth2, il quale permette di accedere ai servizi forniti da applicazioni terze senza fornire a quest'ultime le credenziali di accesso (sulle quali quindi l'utente e Argo continuano ad avere esclusivo controllo).

L'accesso ai servizi BSMART utilizzando le credenziali Argo è naturalmente facoltativo e in caso di accettazione da parte dell'utente, l'utente è reindirizzato dalla piattaforma BSMART ad un dominio Argo, unico punto di accesso da cui viene consentito trasmettere le proprie credenziali Argo.

Al termine del processo di autenticazione, l'utente viene rimandato sul dominio del *client* da cui ha avuto origine la richiesta, e precedentemente autorizzato dalla Argo.

I dati forniti a BSMART si riferiscono esclusivamente a nome, cognome, codice fiscale, indirizzo email, ruolo (docente, genitore o alunno).
Le attività svolte da BSMART nell'erogazione dei servizi di e-learning, anche se accedute con credenziali Argo, sono agite in assoluta autonomia e sotto la responsabilità di BSMART che agisce in qualità di titolare del trattamento.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo 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.

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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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, 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 viaggiono sulla rete criptati, secondo il protocollo SSL che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, la scuola – su richiesta del Dirigente scolastico – può optare per:
- la restituzione e mantenimento dei dati (a fronte di un pagamento di un canone);
- la restituzione e cancellazione/anonimizzazione dei dati.

I dati vengono restituiti in formato aperto, nei tempi tecnici di esportazione sicura dei dati.
Dalla data di cessazione, è consentito l'accesso all'applicazione web da parte degli utenti per un ulteriore periodo di 1 mese.

I tempi tecnici occorrenti alla 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

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.
Per la fornitura dei servizi web, la Argo Software srl 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://www.portaleargo.it/docs/nomina.pdf.
In caso di assenza di nomina formale, la Argo Software si riserva il diritto di sospendere l'erogazione del servizio fino ad adempimento da parte del cliente.

Responsabile per la Protezione dei Dati (DPO) della Argo Software, è Chiara Delaini, raggiungibile all'indirizzo dpo@argosoft.it o dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte della scuola o sospetta violazione di dati.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software 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 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 Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale argo.

Ultimo aggiornamento 05/04/2020

Policy Argo del 20/01/2020

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

Premessa

Il presente documento descrive la policy della Argo Software in materia di sicurezza informatica, continuità operativa e trattamento dei dati personali contenuti negli archivi e nei repository delle scuole fruitrici dei servizi web Argo.

La Argo software srl è impegnata costantemente a migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, 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.

Nell'ambito della continuità operativa, Argo Software adotta tutti gli accorgimenti organizzativi, le soluzioni tecniche e procedurali idonee al 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.).
Da Marzo 2019 la Argo Software è iscritta nell'elenco dei fornitori di servizi SaaS qualificati AgID secondo la circolare N. 3 del 9 aprile 2018.

Il Sistema di Gestione della Sicurezza delle Informazioni di Argo Software srl, nell'ambito dei servizi di progettazione, sviluppo, erogazione, in modalità cloud SaaS e on-premises, è inoltre certificato secondo lo standard ISO/IEC 27001:2017 [certificato n. 556/19 RINA Service S.p.A.].

Tipologia dei dati gestiti dalla Argo Software

I dati gestiti dalla Argo Software riguardano le informazioni (generiche e personali) contenute negli archivi delle scuole fruitrici dei medesimi servizi ed i profili degli utenti fruitori dei servizi web Argo.

In riferimento alle informazioni contenute negli archivi delle scuole, la natura dei dati varia in base alle caratteristiche del servizio attivato dalla scuola. Possono quindi essere conservate informazioni personali e, nel caso di servizi collegati alla gestione del personale e degli alunni, possono essere trattati anche dati appartenenti alle categorie particolari di cui all'art. 9 del Regolamento UE 2016/679 [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 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, proprie clienti, Argo Software 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 alla Argo Software.
Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.
L'accesso ai servizi di amministrazione è eseguito attraverso utenze di dominio nominative.
Con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del personale all'uopo 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

Tutti i dati archiviati sui dischi all'interno di cluster Amazon e tutti i backup in Amazon S3 sono protetti con la crittografia, *mediante l' Advanced Encryption Standard AES-256.*

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Argo, 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, il servizio Amazon RDS 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.
I log delle transazioni per le istanze database vengono caricate in Amazon S3 ogni 5 minuti.

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.
Decorso questo periodo, viene mantenuta una copia settimanale per ulteriori 25 giorni.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web Argo, attraverso il portale Argo, è di esclusiva pertinenza della scuola.

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 e, su richiesta, l'invio di notifiche relative agli accessi effettuati dall'utente all'area di gestione utenza del portale Argo.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente dalla Gestione delle Utenze del Portale Argo, accedendo alla gestione “Anagrafe Utente”. Dietro esplicito consenso da parte dell'utente, l'indirizzo mail potrà essere utilizzato da parte della Argo Software per l'invio di comunicazioni di natura esclusivamente tecnica sull'utilizzo dei programmi Argo a cui l'utente risulta abilitato (faq, guide, videoguide, manuali d'uso, comunicazioni sulle novità riguardanti gli aggiornamenti, nuove soluzioni). L'opzione di scelta per l'invio delle suddette comunicazioni può essere modificata dall'utente in qualsiasi momento sempre dalla gestione "Anagrafe Utente".

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Argo Software s.r.l. esegue il tracciamento degli accessi ai servizi web Argo 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.

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 Argo 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 da società terze, specializzate nel settore della sicurezza informatica, Penetration test e verifiche di Vulnerability Assessment.

Per quanto riguarda l'aggiornamento delle misure di sicurezza, la Argo è iscritta ad un servizio di early warning per il monitoraggio continuo delle vulnerabilità.

Criteri di selezione delle server farm

La Argo Sofware 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, 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 viaggiono sulla rete criptati, secondo il protocollo SSL che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.

Disponibilità dei dati

Per gli applicativi web Argo relativi all'area didattica (Alunni, Scrutini, ScuolaNext, DidUP, Formazione classi prime) e contabile (Bilancio, Project), è possibile richiedere sempre una copia di backup in locale dei dati residenti presso i server Argo. La procedura, totalmente automatizzata, è disponibile all'interno dell'Area Clienti del sito Argo, e consente di scaricare una copia in locale dei dati della scuola residenti in remoto. Per motivi di sicurezza, la richiesta può essere inoltrata dalla suddetta area esclusivamente accedendo con le credenziali dell'amministratore dei servizi della scuola (Supervisor), nella persona del Dirigente scolastico o suo delegato. Una volta processata, i dati sono resi disponibili per lo scarico all'interno dell'area per un periodo di tempo limitato.
All'indirizzo mail comunicato in fase di richiesta, viene inviata la password posta a protezione del file di backup.

Per la restituzione dei dati relative a piattaforme documentali (Gecodoc, Albo Pretorio Online, Amministrazione Trasparente) occorre fare richiesta all'indirizzo assistenza.argo@pec.ecert.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 per 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 web Argo, la scuola – su richiesta del Dirigente scolastico – può optare per:
- la restituzione e mantenimento dei dati (a fronte di un pagamento di un canone);
- la restituzione e cancellazione/anonimizzazione dei dati.

I dati vengono restituiti in formato aperto, nei tempi tecnici di esportazione sicura dei dati.
Dalla data di cessazione, è consentito l'accesso all'applicazione web da parte degli utenti per un ulteriore periodo di 1 mese.

I tempi tecnici occorrenti alla 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

La Argo Software garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, ai sensi dell'art. 28 del Regolamento UE 2016/679.
Per la fornitura dei servizi web, la Argo Software srl 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, la Argo Software mette a disposizione dei clienti anche un modello scaricabile all'indirizzo:
https://www.portaleargo.it/docs/nomina.pdf.
In caso di assenza di nomina formale, la Argo Software si riserva il diritto di sospendere l'erogazione del servizio fino ad adempimento da parte del cliente.

Responsabile per la Protezione dei Dati (DPO) della Argo Software, è Chiara Delaini, raggiungibile all'indirizzo dpo@argosoft.it o dpo-argosoft@ecert.it per qualsiasi richiesta di informazioni da parte della scuola o sospetta violazione di dati.

In qualità di Responsabile del Trattamento dei Dati, la Argo Software 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 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 Argo 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.

Registro delle attività di trattamento

Ad ogni scuola cliente viene garantita la possibilità di accedere al proprio registro delle attività di trattamento elaborato dalla Argo Software in qualità di Responsabile del Trattamento. La funzione è disponibile all'interno del portale Argo (www.portaleargo.it), nella gestione "Profilo scuola", accedendo come Supervisor. All'interno della medesima gestione sono inoltre presenti i campi relativi al Rappresentante legale, al Responsabile per la protezione dei dati e ai dati di contatto di quest'ultimo, compilabili da parte della scuola per consentire di adempiere agli obblighi di informazione intercorrenti tra titolare del trattamento e responsabile del trattamento.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Argo (www.argosoft.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati, delle revisioni del Piano di Business Continuity della Argo Software e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione a tutte le scuole clienti mediante email o avviso sul portale argo.

Ultimo aggiornamento 20/01/2020