Trattamento dei dati nei servizi SAAS e PAAS

Informazioni riassuntive

Responsabile del trattamento					
Denominazione	Ars Edizioni Informatiche Srl				
Partita Iva	13309950155				
Indirizzo	Via Losanna,15				
Città	Milano	**Cap**	20154	**PV**	MI
Legale Rappresentante	Giacomo Balestrini				

Incaricati del trattamento
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti

Dati di contatto		
Responsabile del trattamento	Ars Edizioni Informatiche Srl	privacy@arsedizioni.it 02 3192301

Finalità del trattamento

La Gestione dei dati personali di interessati, studi professionali, aziende finalizzato alla gestione dei dati personali nei singoli applicativi e moduli utilizzati.

Gestione dei documenti generati dai singoli applicativi attraverso un DMS (Document Management System). La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.

Categoria interessati

Dipendenti, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori, visitatori.

Categorie di dati personali

Dati anagrafici di personale dipendente, collaboratori, fornitori appaltatori, visitatori in funzione dell'applicativo che li utilizza.

Dati relativi al rapporto di lavoro con dati economici e dati relativi al contratto di lavoro applicato.

Categorie di destinatari a cui i dati potranno essere comunicati

Incaricati di progettazione e sviluppo software di Ars Edizioni Informatiche finalizzati ad eseguire attività di assistenza e manutenzione.

Trasferimento dati all'estero

NO

Termini per la cancellazione dei dati

I dati conservati nel Data Center Ars Edizioni Informatiche saranno conservati per tutta la durata del contratto e per i 90 giorni successivi alla sua cessazione. Saranno conservati su supporti di backup per i successivi 12 mesi. I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale.

Il Titolare ha la possibilità, attraverso le funzioni applicative, di lanciare cancellazioni massive dei dati personali salvati nel database, solamente entro la durata del contratto.

ARS Edizioni Informatiche declina ogni responsabilità in caso di eliminazione accidentale o meno, data breach o altro incidente informatico o tecnico, riguardo ai dati di Titolari che non hanno un contratto regolare in essere.

Le proroghe per la conservazione dei dati non sono considerate estensioni del contratto.

Descrizione generale delle misure di sicurezza tecniche e organizzative

Misure di sicurezza implementate nei software

Le misure di sicurezza configurabili nel sistema applicativo sono:

Gestione credenziali di accesso

- User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale amministrativa che viene consegnata al titolare e da questo utilizzabile sono in circostanze eccezionali. Il titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione.
- Password: le regole di complessità della password non sono configurabili. È sempre richiesta una password ci complessità alta.
- Disattivazione/disabilitazione credenziali: anche i tempi di disattivazione delle credenziali inutilizzate o la disabilitazione delle credenziali di incaricati che non hanno più le caratteristiche soggettive per accedere a quei dati personali sono configurabili nel sistema da parte del titolare.

Minimizzazione

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.

Identificazione di chi ha trattato i dati

- Strumenti di log: Il Titolare può richiedere i log di tutte le attività eseguite sui dati incluso accessi e operazioni di modifica. I log sono abilitati per default e non possono essere disabilitati dal Titolare.
- I log sono richiedibili entro 45 giorni.
- I log non sono direttamente accessibili dal Titolare.
- Presenza di utenze di servizio per personale di assistenza: Coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali che dovranno essere attivate e disattivate dal Titolare in funzione della necessità.

Tecniche di crittografia

- Crittografia delle password: viene registrato, in luogo della password in chiaro, un valore crittografato con AES256.
- Crittografia della base dati: non disponibile.
- Crittografia file DMS: tutti i documenti generati dalle applicazioni e conservati nel DMS, oppure allegati come documento esterno, sono crittografati con AES256.

Privacy by default

- Attivazione profilo utente: gli utenti nel portale sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale.

Diritti degli interessati

- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che farà le opportune valutazioni. Qualora il Titolare decida che i dati debbano essere cancellati potrà agire direttamente, cancellando l'anagrafica all'interno di ogni applicativo o modulo non sarà più reperibile alcuna informazione neppure indiretta su quell'interessato ad eccezione del nominativo di chi ha eseguito un'attività passata su un dato ancora in uso (storico).

Responsabile del trattamento: misure di sicurezza implementate per i servizi di assistenza

Assistenza tramite ticket/e-mail

L'addetto Ars Edizioni Informatiche non è autorizzato a farsi mandare le credenziali di accesso del Titolare via e-mail né tantomeno potrà salvarle sullo strumento di supporto e ticketing.

Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Ars Edizioni Informatiche è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico Ars Edizioni Informatiche dovrà richiedere credenziali individuali oppure l'utente generico di supporto attivabile\disattivabile dal Titolare.

L'utente di supporto è sempre e solo support@arsedizioni.it ed è attivato di default. Nel caso il Titolare non lo desiderasse, lo dovrà disabilitare.

Utilizzo dei dati presenti nel data base del Titolare

a) L'addetto Ars Edizioni Informatiche che esegue l'assistenza al Titolare è autorizzato ad accedere ai dati del cliente per:
b) Verificare un comportamento non previsto
c) Correggere un errore e verificare l'efficacia della soluzione adottata
d) Sviluppare personalizzazioni

Responsabile del trattamento: misure di sicurezza implementate per i servizi SAAS-PAAS

Riassunto

CODICE	CLASSE	LIVELLO DI APPLICAZIONE
M1	Sicurezza locali e apparati	Le aree tecniche di competenza Ars Edizioni Informatiche sono caratterizzate da misure che controllano l'accesso fisico ai locali.
M2	Autenticazione	I sistemi ed i servizi Ars Edizioni Informatiche sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati.
M3	Sistema di autorizzazione	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti a livello del sistema operativo della piattaforma che ospita l'applicazione (Windows) e a livello applicativo.
M4	Controllo integrità dati	Sono attivi servizi di controllo per presenza di virus sia nei file systems locali dei singoli PC che nei file system condivisi, oltre che sui messaggi di posta elettronica.
M5	Backup e ripristino dati	Sono in atto politiche di backup per i dati. Sono in atto attività indirizzate a ridurre il disservizio in caso di guasto (disaster/recovery)
M6	Gestione delle politiche di sicurezza	Sono predisposte delle Policy IT indirizzate alla sicurezza.
M7	Supporti removibili	Sono disposte regole per la gestione (custodia, uso e riutilizzo) di supporti removibili in presenza di dati sensibili.
M8	Formazione degli incaricati	È previsto un piano di formazione e di aggiornamento per gli incaricati di Ars Edizioni Informatiche.

Dettaglio

CODICE	CLASSE	LIVELLO DI APPLICAZIONE
M1	1.1 Sistemi di allarmi antintrusione	È previsto un sistema di allarme contro le intrusioni. In caso d'intrusione il sistema di allarme procede ad avvisare automaticamente i referenti di Ars Edizioni Informatiche.
	1.2 Controllo accessi ad aree riservate	L'accesso al CED è consentito solamente al personale autorizzato. Il CED è chiuso a chiave e solo il personale autorizzato è in possesso delle chiavi. L'accesso al CED è registrato.
	1.3 Prevenzione incendi	I locali sono dotati di impianti automatici di rivelazione fumo. I locali tecnici prevedono un impianto per lo spegnimento degli incendi. Sono applicate le misure di sicurezza previste dal Dlgs 81/2008.
	1.4 Dislocazione degli apparati attivi e dei server di rete	Tutti gli apparati attivi ed i server di rete sono dislocati in locali tecnici ad accesso controllato.
	1.5 Registrazione accessi agli uffici	Data ed ora di ingresso ed uscita del personale impiegatizio vengono registrati tramite l'ausilio di apparecchi di rilevazione presenze.
M2	2.1 Adozione di procedure di gestione delle credenziali di Autenticazione: USERNAME	Tutti i lavoratori sono identificati nel sistema informativo attraverso una user name assegnata in modo univoco agli stessi. L'accesso ad ogni ambiente o strumento elettronico avviene attraverso credenziali di autenticazione.
	2.2 Adozione di procedure di gestione delle credenziali di Autenticazione: PASSWORD	Ogni utente che inizia un trattamento di dati personali viene edotto sull'importanza che la componente riservata della credenziale di autenticazione non venga divulgata ad altri operatori. Inoltre l'incaricato viene formato sulle regole minime di composizione della password (almeno 8 caratteri e costituita da caratteri alfanumerici non facilmente riconducibili al soggetto di appartenenza). L'incaricato viene inoltre edotto sulla necessità di modifica delle password ogni sei mesi nel caso in cui tratti dati personali e ogni tre mesi qualora tratti dati sensibili (i dati giudiziari non sono stati ad oggi identificati in azienda). Gli strumenti utilizzati per i trattamenti spesso non gestiscono in autonomia il cambio password, né effettuano controlli sulla ripetitività delle stesse password nel tempo. Quindi tali adempimenti sono a carico dello stesso utente.
	2.3 Uso esclusivo delle credenziali di autenticazione	Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo. È compito del cliente eliminare o disabilitare le credenziali di un operatore che non fa più parte della sua organizzazione. È compito e responsabilità del cliente vegliare sulla corretta applicazione delle regole per la non divulgazione delle credenziali. ARS Edizioni Informatiche declina ogni responsabilità inerente alla violazione attraverso credenziali definite e gestite interamente dal cliente.
M3	3.1 Profilo di autorizzazione per singolo incaricato	Detto processo garantisce, a fronte del superamento della fase di autenticazione, la corretta e completa associazione tra utenza ed oggetti del sistema informatico connessi al profilo assegnato; comprende l'insieme delle informazioni, associate ad una persona, dirette ad individuare a quali dati essa possa accedere ed altresì di quali trattamenti essa possa usufruire; esso stabilisce a quali aree del sistema informatico l'incaricato possa accedere e quali azioni, una volta entrato, possa compiere.

CODICE	CLASSE	LIVELLO DI APPLICAZIONE
M4	4.1 Architettura sicurezza informatica	E previsto un insieme di regole comportamentali e procedure operative dirette a proteggere l'intero sistema informatico In particolare, esso prevede l'adozione di programmi diretti a prevenire la vulnerabilità degli strumenti elettronici da un lato contrastando gli attacchi esterni dall'altro provvedendo alla correzione dei difetti insiti negli strumenti stessi. In relazione alla correzione dei difetti, esso opera l'aggiornamento costante dei prodotti e la verifica periodica dell'installazione e della configurazione dei prodotti software. In relazione alla tutela da intrusioni esterne di iniziativa della "mente criminale", l'architettura antivirus si serve di sistemi IDS (Intrusion Detection System), gestiti dal gruppo Sistemistico di Ars Edizioni Informatiche, diretti ad individuare qualunque tentativo di operare e/o introdursi illecitamente nella rete e nei sistemi posti sotto protezione. È attivo un sistema antivirus che monitorizza tutta la rete aziendale. Il sistema è attivo sia sui desktop che sui laptop. L'antivirus si aggiorna tutte le volte che la casa produttrice aggiorna la lista delle segnalazioni virus. L'ufficio tecnico, qualora ritenga che a seguito di richiesta di un operatore, il sistema possa essere infetto, lancia la scansione per verificare eventuali infezioni. I laptop sono muniti di sistema antivirus che si aggiorna tutte le volte che il laptop si collega alla rete aziendale. Vi è un sistema di firewall che filtra le comunicazioni in entrata e in uscita.
M5	5.1 Procedure di backup	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera.
	5.2 Procedure di ripristino	Sono adottate idonee misure atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli interessati e non superiori a sette giorni. Sono altresì previste attività indirizzate a ridurre il disservizio in caso di guasto.
M6	6.1 Policy per l'utilizzo degli strumenti IT	Sono predisposte policy per l'utilizzo degli strumenti elettronici relativamente agli aspetti di: - Utilizzo del Pc - Navigazione Internet - Utilizzo della posta elettronica
M7	7.1 Istruzioni agli incaricati	Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
	7.2 Custodia, uso e riutilizzo supporti rimovibili	I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intellegibili e tecnicamente in alcun modo ricostruibili.
M8	8.1 Piano di Formazione degli incaricati	E' prevista una formazione per tutti gli incaricati di Ars Edizioni Informatiche.

Responsabile del trattamento: misure di sicurezza applicate al data center

- *Certificazioni*: Ars Edizioni Informatiche ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. Certificazioni: ISO 27001.
- *Compliance*: i processi aziendali di Ars Edizioni Informatiche rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate Ars Edizioni Informatiche adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.
- *Accesso alle informazioni*: il sistema di gestione di Ars Edizioni Informatiche prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare, i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.
- *Accesso ai sistemi*: gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da Ars Edizioni Informatiche o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'acquisizione di dati. Gli accessi di amministrazione da parte di Ars Edizioni Informatiche sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.
- *Sicurezza dei sistemi*: i servizi di sicurezza si ritengono attivi e funzionanti a protezione delle componenti ospitate in Datacenter. I sistemi di protezione sono progettati in modo da massimizzare la protezione e sono amministrati da personale

con formazione specifica che segue procedure operative stringenti.

- *Controlli di sicurezza*: sull'intera infrastruttura Datacenter sono svolti Penetration Test e Vulnerability Assessment con cadenza annuale
- *Firewalling*: il networking del Datacenter è separato dalle reti pubbliche, dalle altre reti di Ars Edizioni Informatiche e dalle altre reti del cliente. I flussi dati tra il networking del Datacenter e l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.
- *Intrusion Prevention*: il Datacenter è protetto da sistemi di Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito e si comportano in modo trasparente nei confronti del traffico legittimo.
- *Filesystem Antivirus*: tutti i server dispongono di moduli Antivirus sul filesystem e, su base progettuale, possono essere configurati prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.
- *Security Patch Management:* la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dal produttore e ritenute critiche per l'erogazione del servizio o per la sicurezza. L'applicazione delle patch verrà sottoposta a preventiva comunicazione al cliente e la schedulazione avverrà in accordo con quest'ultimo.
- *Continuità ed emergenza*: il Datacenter è stato concepito per fornire affidabilità massima in termini di alimentazione dei server, in quanto ogni rack è connesso a due alimentazioni indipendenti (quadri elettrici attestati su UPS ridondati), in modo tale da permettere la manutenzione delle singole linee di alimentazione senza creare disservizio e di scongiurare blackout nel caso di fault di una linea di alimentazione.
- *Linee di comunicazione*: le soluzioni ed i servizi proposti possono essere erogati tramite connessione Internet protetta (https). Il cliente potrà scegliere di predisporre a propria cura e spese una linea di comunicazione VPN o MPLS.