Information Security Policy Document (ISPD)

01.CP_06 – 25/03/2023

Scopo del documento

Il presente documento ha lo scopo di definire la politica per la sicurezza delle informazioni che Archiva Srl, nel suo ruolo di Conservatore, oltre che Intermediario finanziario versi lo SDI e Titolare, Responsabile (o altro responsabile) ex art. 28 Regolamento (UE) 2016/679.

Archiva Srl ha implementato un Sistema di Gestione Integrato (IMS), comprendente un Sistema di Gestione della Sicurezza delle Informazioni secondo lo standard tecnico ISO/IEC 27001:2013 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti), avente come ambito di certificazione la *"Progettazione, sviluppo e manutenzione ed erogazione di servizi e prodotti software in modalità SaaS, di fatturazione elettronica, conservazione di documenti informatici, tramite tecniche di firma elettronica, dematerializzazione di archivi cartacei mediante l'applicazione delle Linee guida ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701. Soluzioni di firma elettronica".*

Nota 1: ISO/IEC 27017 (Information technology - Security techniques - Code of practice for information security controls based on ISO/IOEC 27002 for cloud services);

Nota 2: ISO/IEC 27018 (Information technology - Security techniques - Code of practices for protection of personally identifiable information (PII) in public cloud acting as PII processors);

Nota 3: ISO/IEC 27701 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

Questo documento è efficace anche per quanto richiesto dal consorzio ENX a proposito della certificazione TISAX.

Riferimenti normativi

Norma	Clausola
ISO/IEC 27001 , ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701	5.1 5.2 CLD.6.3.1
Linee guida sulla formazione, gestione e conservazione di documenti informatici.	3.9, 4.10
ISO 22301	5.2.1
UNI PdR 43.2	6.3.3
Regolamento (UE) 2016/679	art. 32
Regolamento (UE) 910/2014	art. 10
TISAX	1.1.1

Termini e definizioni

Ai fini del presente documento, si applicano i termini e le definizioni date in:

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

- Regolamento (UE) 2016/679;
- Regolamento (UE) 2018/1807;
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici. (AgID)

Introduzione

Lo scopo della Information Security Policy Document (ISPD) è quello di salvaguardare la sicurezza delle informazioni, le persone, le società, le organizzazioni e nazioni che in qualsiasi misura interagiscono con Archiva Group, dai rischi di sicurezza delle informazioni e dai rischi cyber.
Questa politica informa tutti gli stakeholders (interni ed esterni) sui principi guida rilevanti per l'intero ciclo di vista dei dati ex. Regolamento (UE) 2016/679 e Regolamento (UE) 2018/1807. Tutti i fornitori di Archiva Group coinvolti nell'erogazione dei servizi di Archiva sono tenuti al rispetto della presente politica e all'implementazione di analoghe disposizioni.

L'obiettivo di Archiva group è che:

- le informazioni siano protette dall'accesso non autorizzato o dall'uso improprio;
- la riservatezza delle informazioni sia garantita;
- l'integrità delle informazioni sia mantenuta;
- i concetti di cybersecurity (identify, protect, detect, respond e recover) sia recepiti, implementati e costantemente monitorati e aggiornati;
- la disponibilità delle informazioni e dei sistemi informativi sia mantenuta per l'erogazione dei servizi;
- siano mantenuti i processi di pianificazione e attuazione della continuità operativa;
- siano rispettati i requisiti normativi, contrattuali e legali;
- sia mantenuta la sicurezza fisica, logica, ambientale e delle comunicazioni.

La violazione di questa Politica può comportare, per il trasgressore, azioni disciplinari o azioni penali.

Quando le informazioni non sono più utili, vengono smaltite adottando le indicazioni contenute nella norma UNI CEI ISO/IEC 21964:2020.
Tutti gli incidenti relativi alla sicurezza delle informazioni verranno segnalati al CISO e, laddove pertinente anche al DPO, e indagati secondo le procedure interne definite in conformità a requisiti di certificazione.

Obiettivi

Con l'obiettivo di definire le linee di indirizzo aziendale riguardanti la protezione dei dati, sulla base della loro classificazione in termini di Riservatezza, Integrità, Disponibilità e prova, demandando a specifiche procedure ed istruzioni operative, laddove applicabile, l'indicazione dei processi operativi necessari per la classificazione delle informazioni stesse, sono individuati i seguenti obiettivi:

- obiettivi strategici:
    - perseguire e mantenere la conformità normativa circa la sicurezza delle informazioni;
- obiettivi tattici:

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

- definire linee di indirizzo generali applicabili in tutti i contesti aziendali, alla sicurezza delle informazioni, qualità, Data Protection e privacy;

- obiettivo operativo:
  - avviare la redazione e pubblicazione e periodica revisione di procedure e istruzioni operative necessarie per il conseguimento dei più generali obiettivi tattici e strategici.

Il presente documento è reso disponibile a tutta l'azienda, attraverso i sistemi informativi adottati, e mantenuto periodicamente aggiornato sulla base dei necessari adeguamenti normativi e tecnologici che tempo per tempo si rendono necessari.

Obiettivi e principi guida

Archiva Srl attribuisce primaria importanza alla sicurezza delle informazioni, lavorate per conto dei propri clienti o trattate in prima persona, in considerazione dei crescenti trend di minacce e vulnerabilità, della difficoltà di manette nel tempo efficaci misure di sicurezza, ed in fine della cultura aziendale e sensibilità del personale coinvolto nelle operazioni di business.

Per questo motivo sono identificati i seguenti principi elementari:

- la **formazione del personale** è elemento essenziale per prevenire il manifestarsi di indesiderate situazioni avverse che possono risultare in danno all'azienda ed agli stakeholders coinvolti;
- la **formazione specifica** nella progettazione di servizi, processi ed applicazioni è elemento indispensabile per garantire l'implementazione di soluzioni che possano corrispondere alle reali necessità dl cliente, nel rispetto delle più accreditate linee guida e prassi di riferimento.
- il **continuo monitoraggio** di minacce e vulnerabilità è essenziale per garantire la sicurezza ed efficacia dei sistemi e dei servizi erogati ai clienti;
- la **continua valutazione** delle misure di sicurezza adottate è essenziale per garantire a tuti gli stakeholders il mantenimento dei requisiti minimi di sicurezza delle informazioni;

Archiva Srl attribuisce ha inoltre stabilito i seguenti obiettivi specifici:

Qualità dei Servizi e dei Prodotti

Archiva eroga Servizi e Prodotti coerenti con le esigenze, le aspettative e le necessità del Cliente.

I nostri Servizi e Prodotti seguono severe procedure di sviluppo e di verifica dei requisiti. La nostra promessa di qualità non si esaurisce alla consegna di quanto previsto dal Contratto ma è basata su un continuo miglioramento sia lato Servizio/Prodotto che lato procedurale. Gli stessi step di verifica e approvazione interna dei requisiti sono in continuo monitoraggio ed aggiornamento, per garantire che anche i canoni di valutazione siano coerenti con le evoluzioni normative, tecnologiche e di mercato.

Il nostro personale viene formato in modo continuativo con uno spiccato tratto consulenziale. Un approccio basato sull'ascolto del Cliente. Un atteggiamento propositivo e proattivo garantisce la coerenza di servizi personalizzati e strutturati sulle reali esigenze del Cliente, slegati da logiche di mero interesse commerciale o da approcci tecnologici pregiudiziali.

La gestione di una comunicazione informativa e formativa puntuale, gratuita e riservata ai clienti e agli utenti dei nostri Servizi, completa la nostra ricerca di eccellenza qualitativa, creando un ponte collaborativo tra Archiva, Cliente e utilizzatore, il cui senso finale risiede nella volontà di fornire soluzioni efficaci e velocemente implementabili in un contesto di mercato fortemente liquido e mutevole.

Archiva è azienda certificata ISO 9001.

Archiva potrà richiedere al Cliente di rispondere ad un questionario sulla qualità dei servizi erogati.

Definizione degli obiettivi per la gestione ambientale e pianificazione per il loro raggiungimento

Il Gruppo Archiva ("Archiva Group") definisce gli obiettivi di gestione ambientale e pianifica il loro raggiungimento: ciò permette il conseguimento degli obiettivi strategici, l'implementazione delle politiche di gestione ambientale e la misurazione di indicatori di performance dell'IMS (Integrated Management System).

I risultati della valutazione dei rischi ambientali e della fase di trattamento del rischio sono usati come input per la revisione degli obiettivi, al fine di assicurare che questi ultimi rimangano appropriati alle circostanze dell'organizzazione.

Gli obiettivi di seguito indicati sono:

- consistenti con la politica per la gestione ambientale;
- misurabili, quando è possibile determinare - secondo un certo criterio - quando l'obiettivo è raggiunto;
- collegati agli aspetti ambientali pertinenti individuati nella politica per la gestione ambientale;
- monitorati, comunicati e - quando necessario - aggiornati.

L'erogazione dei servizi applicativi interni ad Archiva Group, così come quelli destinati ai propri clienti, sono ispirati alle migliori pratiche di gestione ambientale per il settore TIC (Tecnologie dell'Informazione e Comunicazione).

Archiva Group attraverso la certificazione ISO 14001, stabilisce i seguenti obiettivi:

1) miglioramento della gestione ambientale, attraverso investimenti nella struttura, nei mezzi, nelle attrezzature informatiche e nella formazione del personale interno;

2) valutazione di diverse alternative per il rinnovo del parco auto aziendale in linea con la politica per la gestione ambientale;

3) approvvigionamento di energia elettrica per l'erogazione dei servizi di business e per la sede operativa di Archiva Group, esclusivamente da fonti rinnovabili;

4) allineamento agli obiettivi dell'Agenda 2030 per lo Sviluppo Sostenibile.

Sicurezza delle informazioni

Garantiamo su base permanente il mantenimento di integrità, riservatezza e disponibilità dei dati (personali e non) trattati per conto dei Clienti.

In Archiva la sicurezza delle informazioni oltre che dovere diviene priorità.

Archiva eroga i propri Servizi garantendo al cliente il massimo livello di sicurezza delle informazioni grazie ad un'infrastruttura solida ed efficace nel pieno rispetto dei principi di riservatezza, integrità e disponibilità dei dati enunciati nella certificazione ISO/IEC 27001.

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Le integrazioni ISO/IEC 27017 e ISO/IEC 27018 ci obbligano a controlli avanzati in qualità di fornitori di servizi in cloud e ad applicare una rigida condotta per la protezione delle PII ("Personally Identifiable Information") nei servizi in cloud.

Infine, l'integrazione ISO/IEC 27701 e il raggiungimento della certificazione UNI PdR 43.2 garantisce un pieno recepimento degli obblighi in capo ad Archiva in qualità di Titolare e/o Responsabile del trattamento, agevolando il futuro percorso di certificazione verso il GDPR.

Con dato ACCREDIA, Archiva si posiziona come una tra le aziende più certificate in Italia.

I servizi erogati devono quindi soddisfare i requisiti di molti quadri normativi imponendo un approccio volto al miglioramento continuo per garantire la sicurezza dei vostri dati e la continuità operativa del Servizio.

Il nostro sistema di gestione integrato (IMS) armonizza e implementa in maniera omogenea i diversi requisiti imposti dalla normativa internazionale, che coprono sia il lato procedurale che tecnologico.

Continui investimenti in formazione e informazione del nostro personale, garantiscono che tutti i collaboratori Archiva abbiano le competenze e conoscano le procedure per prevenire "Incident", sia in ambito "Data Protection" che "Information Security".

Continuità operativa

Garantiamo che l'erogazione dei servizi applicativi sia supportata da soluzioni ridondate, in alta affidabilità, non solo sul sito primario di Archiva, ma anche a livello geografico.

Archiva attraverso la certificazione ISO 22301, si obbliga ad un insieme di procedure e buone pratiche relative alla gestione della continuità operativa, definendo i requisiti necessari a pianificare, stabilire, attuare, rendere funzionante un sistema di gestione documentato, per monitorare, mantenere attivo e migliorare in continuo il sistema di gestione finalizzato a proteggere, ridurre le possibilità di accadimento, preparare, dare risposte e ripristinare eventi destabilizzanti per un'organizzazione, quando questi abbiano a manifestarsi.

Il sistema di gestione per la "Business Continuity" di Archiva è per noi un'evoluzione del Sistema di Gestione della Qualità ISO 9001.

Se la ISO 9001 ci aiuta nella gestione delle attività in "ordinaria amministrazione", il Business Continuity Management garantisce il mantenimento, il recupero e il ripristino dei servizi dopo eventi di interruzione gravi.

Prevenzione della corruzione

Archiva ha adottato un Sistema di Gestione per la Prevenzione della Corruzione in linea con lo standard internazionale ISO 37001 e si è prefissata il raggiungimento dei seguenti obiettivi:

1. sensibilizzazione e formazione del personale dipendente e delle società controllate
2. sensibilizzazione dei soci in affari e maggiore attenzione nella scelta degli stessi
3. incoraggiamento alle segnalazioni di potenziali fatti corruttivi, anche mediante la messa a disposizione di specifici strumenti di denuncia in forma anonima
4. impegno al miglioramento continuo delle attività dirette alla prevenzione della commissione di atti corruttivi, anche grazie al supporto di una nominata Funzione di Conformità per la Prevenzione della Corruzione ("RCAC").

Ruoli e responsabilità

La matrice sotto riporta i ruoli e le responsabilità assegnate a ciascuna fase del ciclo di vita del presente documento.

Attività	Responsabile	Esecutore	Consultato	Informato
Redazione, pubblicazione	Direzione aziendale	CISO	Line manager, DPO	HR
Adozione	Line manager	Stakeholder interni e esterni		
Revisione	Direzione aziendale	CISO	Line manager, DPO	HR

Direzione aziendale

La Direzione Aziendale ha la responsabilità complessiva della definizione dei principi generali che regolano la sicurezza delle Informazioni e la loro efficace traduzione in procedure operative interne, necessarie a soddisfare garantire il corretto funzionamento dei processi operativi stessi oltre che la conformità al quadro normativo di riferimento e i requisiti contrattuali pattuiti.

CISO

Il Chief Information Security Officer è il responsabile della manutenzione del presente documento. La redazione di specifiche ulteriori politiche, procedure ed istruzioni operative è demandata alle singole funzioni aziendali, volta per volta interessate.

DPO

Il DPO (Responsabile per la protezione dei dati) nell'ambito del presente documento ha il compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono le attività di trattamento circa gli obblighi derivanti dal presente documento, dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Il DPO ha inoltre il compito di sorvegliare l'osservanza del presente documento per quanto attiene al trattamento dei dati personali e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Line manager

I Line manager sono responsabili per la traduzione dei principi definiti attraverso la presente politica all'interno dei propri reparti e dei processi da essi governati. I Line manager sono altresì responsabili dell'applicazione del presente documento da parte dei propri fornitori.

Utenti interni

Gli utenti interni (dipendenti/collaboratori) trattano le informazioni sulla base di istruzioni e autorizzazioni definite in base a specifici profili operativi. Gli utenti interni sono responsabili per l'adozione di misure comportamentali in linea con i principi definiti all'interno del presente documento di politica e con le Istruzioni Operative per gli Autorizzati al trattamento dei dati redatte ex. art. 29 del Regolamento (UE) 2016/679. Agli utenti interni è richiesta inoltre la conoscenza ed il rispetto del Regolamento Aziendale e del Regolamento Informatico. Ogni comportamento in violazione di quanto sopra sarà volta per volta valutato dalla Direzione Aziendale, la quale si riserva fin da ora la possibilità di ricorrere ad azioni disciplinari per quanto già previsto dal CCNL di riferimento.

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

OGNI DIPENDENTE E COLLABORATORE DI ARCHIVA, AL PARI DI UTENTI ESTERNI AI QUALI PER SPECIFICHE RAGIONI VIENE CONCESSO L'ACCESSO AI SISTEMI INFORMATIVI AZIENDALI, È TENUTO A RISPETTARE LE DISPOSIZIONI DELLA PRESENTE POLICY DI SICUREZZA DELLE INFORMAZIONI.

LA VIOLAZIONE DI QUESTA POLITICA E DEI REQUISITI DI SICUREZZA DA QUESTA DISCENDENTI, POTRÀ RISULTARE IN DANNO ALL'AZIENDA LA QUALE SI RISERVA FIN DA ORA LA FACOLTÀ DI INTRAPRENDERE PROVVEDIMENTI DISCIPLINARI O AZIONI LEGALI NELLE OPPORTUNE SEDI.

Principali risultati attesi

L'introduzione della presente politica pone le basi per la definizione di ulteriori politiche, procedure e istruzioni operative, le quali sono fin da ora ispirate ed informate dei principi generali qui definiti, con la cui applicazione l'Azienda vuole garantire il raggiungimento degli obiettivi strategici sopra citati.

Relazioni con altre politiche

Alla presente politica è implicitamente collegata ogni altra ulteriore politica implementata da Archiva.

Considerazioni specifiche per l'erogazione di servizi in cloud e per il trattamento di dati personali nel cloud

A partire dal 2019, Archiva ha avviato un percorso di avvicinamento all'erogazione dei servizi resi a clienti, tramite il cloud. Archiva ha ora adottato un modello "**Multi-tenant SaaS application**", schematizzato nell'illustrazione seguente: (immagine tratta dalla circolare AgID n° 3 del 9 aprile 2018)

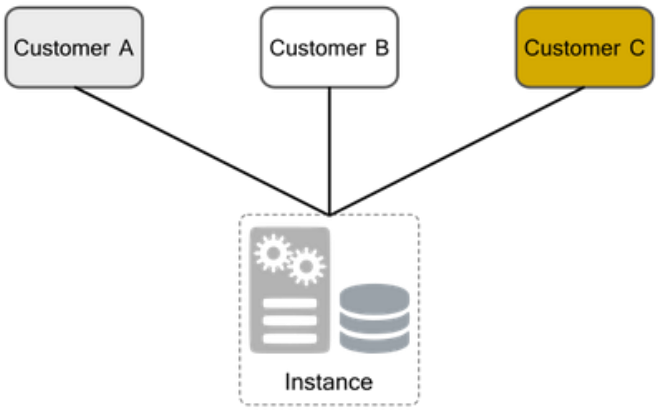

Figura 1: immagine tratta dalla circolare AgID n° 3 del 9 aprile 2018

Una singola istanza applicativa serve contemporaneamente più clienti, i quali accedono alla medesima istanza applicativa in esecuzione su risorse virtuali condivise. L'isolamento dei dati e degli utenti avviene a livello applicativo, di gestione delle basi di dati (DBMS) e degli storage, utilizzando gli opportuni meccanismi di autenticazione, autorizzazione e sicurezza.

Nel percorso di rinnovamento della propria infrastruttura, orientato al Cloud, il nuovo modello, di seguito illustrato, permetterà di avere configurazioni più flessibili.

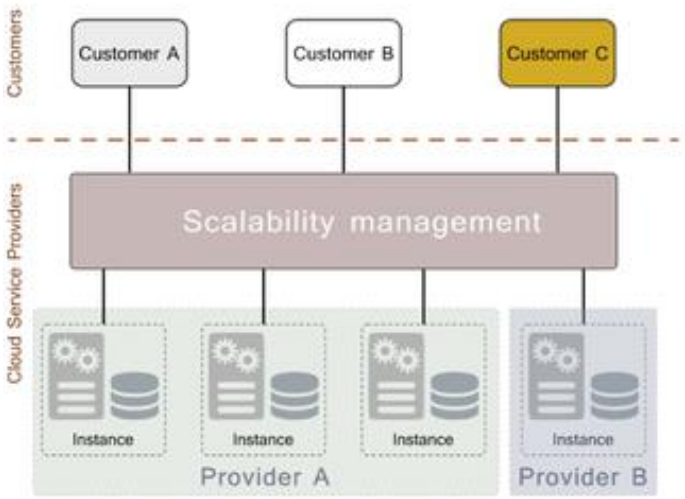

Figura 2:immagine tratta dalla circolare AgID n° 3 del 9 aprile 2018

I clienti potranno avere la loro istanza applicativa in esecuzione su risorse condivise o dedicate (o un misto delle due) in maniera trasparente e configurabile. Il sistema di load balancing permette di implementare le politiche di allocazione (delle nuove istanze applicative) in funzione di una moltitudine di criteri (uno dei più importanti è la qualità del servizio). Le istanze applicative potranno essere aggiunte e rimosse dinamicamente in qualunque momento ed in base alle esigenze. Anche le risorse virtuali necessarie alle applicazioni sono allocate in modo dinamico. L'allocazione di nuove istanze applicative o di risorse virtuali non richiede nessuna modifica architetturale del sistema che è già stato realizzato in modo da adattarsi dinamicamente. Tutto ciò permette di offrire ed attuare SLA diversificati per i vari clienti.

La *baseline* di sicurezza di Archiva, si estende quindi ai controlli di sicurezza delle linee guida sopra citate, le quali devono dunque essere tenute in considerazione per quanto dichiarato nello *scope* di certificazione, con particolare riferimento alla progettazione ed allo sviluppo di prodotti finalizzati alla realizzazione di servizi che verranno erogati tramite il cloud.

Questa nuova prospettiva richiede inoltre che:

- le attività di Risk Assessment tengano maggiormente in considerazione i rischi derivanti da attività seguite da autorizzati all'interno di Archiva;
- sia verificata la segregazione logica e, dove pertinente, fisica degli ambienti applicativi concessi in uso ai clienti;
- sia sempre verificata la possibilità di accesso alle informazioni (asset) dei clienti, ospitate e trattate in ambito cloud;
- sia periodicamente verificata ed aggiornata la procedura di comunicazione verso i clienti, in occasione dell'applicazione di change;
- sia periodicamente verificata la sicurezza degli ambienti virtualizzati su cui si base l'infrastruttura cloud;
- sia periodicamente eseguito un processo di rivalutazione delle utenze concesse in uso ai clienti;

- sia prevista la comunicazione di databreach ed il supporto alle attività investigative connesse.

Tutti i servizi erogati in cloud, sono sotto il controllo della struttura Archiva Information Security" (cfr. HLP_02 Leadership). In sede di sottoscrizione del contratto di servizio con i clienti, è definito il responsabile per il contratto e per l'esecuzione del contratto. Al termine della fase di progettazione del servizio, la funzione Project Management comunica alla funzione Customer Care, i riferimenti del cliente per le successive ed eventuali attività di assistenza.

Archiva si impegna a osservare, fra le aktre, la normativa tempo per tempo vigente in materia di Data Protection & Privacy. Su base volontaria Archiva ha deciso di intraprendere un percorso di certificazione che possa supportare l'azienda nel dimostrare il proprio impegno nel corretto recepimento del Regolamento (UE) 2016/679. A tal fine Archiva ha conseguito la certificazione rispetto la UNI PdR 43.2:2018 - Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT.

Controlli Crittografici

In considerazione della attività proprie di intermediario verso il SDI e di Conservatore, iscritto al Marketplace AgID Conservatori, da cui discendono i conseguenti vincoli generali, di qualità, di sicurezza e organizzativi, Archiva al fine di proteggere i dati trattati per conto dei propri Clienti quando questi sono a riposo, può adottare meccanismi crittografici, in base a quanto concordato in sede di redazione del progetto. Archiva si è dotata di una procedura interna "POA 27 Utilizzo della crittografia", contenente ulteriori elementi generali dei sopracitati meccanismi crittografici a protezione dei dati in transito.

Gestione del Cambiamento

Tutte le modifiche maggiori apportate ai servizi erogati ai clienti, devono essere preventivamente comunicate indicando la data di applicazione di tali modifiche, la loro descrizione e eventuali impatti sull'operatività dei clienti. Archiva ha implementato un processo di gestione dei cambiamenti, governato dalla procedura interna “POA 24 Change Management Procedure”.

Backup

Archiva implementa diverse soluzioni di backup specifiche per i dati trattati e per gli ambienti server virtuali, utilizzati nell'erogazione dei servizi applicativi.

Archiva implementa 2 diversi sistemi di backup:

- Veeam Backup & Replicator per Database, Server ed application server;
- SnapMirror e Snapvault per i documenti, coadiuvato anche da Snapshot Copy.

Le copie di backup sono posizionate all'interno della server-farm presso la sede legale e operativa di Archiva Srl in Villafranca di Verona, e replicate all’interno di un proprio ambiente AWS in Cloud, localizzato presso la region “Milano” in Siziano (PV), con ulteriori repliche, per aspetti di business continuity,presso i poli tecnologici di Cornaredo (MI), Ponte San Pietro (BG) e Siziano (PV). Archiva ha implementato un processo di gestione dei backup, governato dalla procedura interna “POA.SYS.13 Procedura di gestione dei backup/restore”.

Logging e monitoraggio

Archiva mantiene log delle varie componenti che concorrono alla definizione della propria infrastruttura, comprendendo sia apparati di rete, sia elementi software. Archiva ha inoltre implementato un sistema di alerting proattivo che notifica ad una distribution list interna, eventuali circostanze rilevanti. I sistemi di monitoraggio e di conseguenza i sistemi di alerting collegati si distinguono in:

- monitoraggi di misure infrastrutturali, dove l'oggetto della misura sono parametri macchina e che consentono quindi misure operate sui sistemi Hardware quali ad esempio Storage, Processi Server, Apparati di Rete, Connettività, Processi Windows e Demoni Java.
- monitoraggio funzionale applicativo, dove l'oggetto della misura sono l'esecuzione di processi funzionali quali ad esempio la richiesta di visualizzazione di un documento, la messa in conservazione di un pacchetto di versamento, la trasformazione di dati, il login di autenticazione ad una applicazione web.

Maggiori dettagli sulla strutturazione del sistema di logging e monitoraggio adottato da Archiva, sono contenuti all'interno della POA 26 Log e Monitoring del SdC.

Clock Syncronization

Tutti i server utilizzati da Archiva Srl utilizzano il riferimento temporale offerto dall'I.N.RI.M (Istituto Nazionale di ricerca metrologia) tramite protocollo NTP per la sincronizzazione dei propri orologi.

I clienti di Archiva possono sincronizzare i propri sistemi informativi, utilizzando i medesimi server NTP, elencati all'interno del sito web https://www.inrim.it/node/643

Gestione delle Vulnerabilità tecniche

Al fine di monitorare le vulnerabilità tecniche che nel corso dell'erogazione dei servizi applicativi ai clienti possono manifestarsi, Archiva ha adottato un processo ispirato alla norma ISO 30111:2019 - Information technology — Security techniques — Vulnerability handling processes.

Nel corso di un anno solare, Archiva pianifica almeno 4 sessioni distinte di Vulnerability Assessment sul perimetro esterno, esposto su internet, e scansioni sul perimetro interno. Eventuali vulnerabilità critiche sono immediatamente analizzate e la loro remediation è pianificata entro 15gg.

Misure

Archiva, nell'esercizio delle attività in qualità di responsabile del trattamento, adotta come *base line* di sicurezza i controlli indicati nell'annex A della ISO/IEC 27001. Tali controlli, estesi anche alle linee guida ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 27701, sono valutati annualmente in occasione degli audit interni e degli audit di terza parte.

Security Operation Center - SOC

Al fine di garantire su base permanente livelli di sicurezza adeguati, Archiva ha implementato un SOC avvelendosi della collaborazione di un fornitore esterno specializzato che monitora H24, 7x7 tutta l'infrastruttura IT di Archiva e la sua web exposure, al fine di fare emergere eventuali tracce di attività malevole nel darkweb e nel deepweb.

Dati di Test

Nel caso in cui le parti si accordino per l'effettuazione di test funzionali e prestazionali, c.d. "User Acceptance Test", per validare la corretta predisposizione dei Servizi, verranno utilizzati esclusivamente dei dati di test ricevuti dal Cliente. Conseguentemente, tutti i dati ricevuti nella fase di sviluppo del progetto verranno considerati dati di test e non soggetti alla normativa nazionale e sovranazionale a tutela delle persone fisiche con riguardo ai dati personali. Pertanto, tali dati verranno rimossi dai sistemi di Archiva al termine dell'attività di predisposizione del Servizio.

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Responsabilità e procedure

Il cliente, qualora nella fruizione dei servizi applicativi dovesse riscontrare anomalie o rilevare eventi che possono avere ripercussioni sulla sicurezza delle informazioni trattate da Archiva oppure direttamente incidenti di sicurezza delle informazioni, può segnalare ogni circostanza e/o evento scrivo all'indirizzo email security@pec.archivagroup.it oppure, in alternativa, ciso@archivagroup.it. Ogni richiesta di assistenza relativa alla friuzione dei servizi erogati da Archiva può essere inoltrata tramite portale di ticketing https://archivagroup.atlassian.net/servicedesk/ oppure scrivendo all'indirizzo email ticket.care@archivagroup.it.

Tutte le segnalazioni aperte tramite portale sono tracciate all'interno dei sistemi Archiva con uno specifico ticket. Tutte le segnalazioni di eventi di sicurezza delle informazioni , sono tracciate in apposito registro. Per gli eventi, classificati come incidente di sicurezza delle informazioni, oppure databreach, è disponibile un incident report.

Raccolta di evidenze

Archiva mantiene all'interno dei propri sistemi informativi evidenze della corretta implementazione del sistema di gestione integrato a supporto delle attività in ambito di certificazione. Archiva assicura la massima collaborazione con i clienti per permetter loro di rispondere ad eventuali attività di verifica e ispezione, richieste in prima persona o da autorità di controllo, pur tutelando la riservatezza di particolari aspetti tecnologici, implementativi e procedurali, propri di Archiva.

Aspetti specifici per ISO/IEC 27018 e ISO/IEC 29100 - Principi di Protezione dei Dati

Consent and choice

Archiva, in qualità di responsabile del trattamento, come definito nell'atto di designazione sottoscritto per tale ruolo, si obbliga a supportare il Titolare nel rispetto di ogni suo vincolo regolamentare.

Purpose legitimacy and specification

Il trattamento dei dati operato da Archiva, avviene per le sole finalità e secondo le modalità, concordate con il Titolare, nell'atto di designazione a Responsabile del trattamento.

Collection limitation

Archiva, nel ruolo di responsabile del trattamento, non ha la facoltà di scegliere l'insieme dei dati personali da trattare, poiché questi vengono forniti direttamente dal Titolare del trattamento.

Data minimization

Archiva si impegna ad utilizzare solamente i dati strettamente necessari per le finalità dichiarate e ad eliminare dai propri sistemi informativi eventuali file temporanei o documenti di lavoro, non più necessari al trattamento dei dati del Titolari.

Use, retention and disclosure limitation

Archiva prevede la possibilità di dare accesso ai dati del Titolare, su richiesta delle autorità di controllo competenti, senza ritardarne l'accesso ed informando tempestivamente il Titolare, così come previsto nell'atto di designazione a Responsabile del trattamento. Di questa diffusione viene tenuta traccia in apposita documentazione.

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Openness, transparency and notice

Archiva rende noto l'eventuale ricorso ad ulteriori responsabili (come identificati all'Art. 28, comma 4 del Regolamento UE 2016/679), comunicando il loro coinvolgimento, nell'atto di designazione a Responsabile del trattamento.

Accountability

Archiva, in qualità di responsabile del trattamento, si obbliga a notificare al Titolare eventuali violazioni dei dati personali di sua pertinenza, secondo le modalità e le tempistiche definite nell'accordo di designazione a Responsabile del Trattamento. In caso di Data Breach, Archiva redige uno specifico rapporto la cui struttura corrisponde a quanto indicato all'art. 33 del Regolamento (UE) 2016/679.

Al fine di supportare nel tempo eventuali indagini forensi, Archiva mantiene all'interno dei propri sistemi informativi copia aggiornata e storicizzata di tutte le politiche, procedure e istruzioni operative necessarie all'esercizio del Sistema di Gestione Integrato.

Qualora il Titolare richiedesse la restituzione dei propri asset informativi (i documenti conservati all'interno del SdC) Archiva applicherà quanto previsto nella procedura POA 01 - Gestione dello Scarto dal Sistema di Conservazione.

Information security

- tutto il personale dipendente ed eventuali collaboratori di Archiva, sono soggetti a specifici accordi di riservatezza;
- al fine di prevenire la copia non autorizzata di informazioni su dispositivi mobili o trasportabili, Archiva adotta meccanismi di DLP, che segnalano tempestivamente eventuali tentativi di copia non autorizzata;
- tutte le attività di *Restore* dei dati sono tracciate in appositi log applicativi;
- i dati trasmessi dal Titolare non sono memorizzati su dispositivi mobili o rimovibili, eccezion fatta per i casi in cui sia il Titolare a richiedere una copia su supporto ottico di tali dati. In queste circostanze i dati vengono memorizzati all'interno di directory compresse e protette con password robuste, comunicate al Titolare con canali di comunicazione differenti rispetto quello impiegato per la trasmissione dei dati;
- tutti i dati in transito, fra Titolare e Archiva, sono scambiati attraverso canali di comunicazione cifrati (SSL/TLS1.2);
- la distruzione degli originali analogici o delle loro copie, trasmesse dai Titolari, avviene per mezzo di un sub-fornitore contrattualizzato, che esegue il servizio di "macero carta", certificato;
- ogni utente che accede ai sistemi informativi di Archiva, attraverso i quali sono erogati i servizi di business ai Titolari, utilizza credenziali di autenticazione uniche, non generiche non tecniche;
- periodicamente è riesaminata la lista delle utenze autorizzate ad accedere al Sistema di Conservazione;
- le utenze scadute e/o disattivate, non vengono riassegnate ad altri utenti;
- l'atto di designazione a Responsabile del trattamento, indica le misure minime di sicurezza implementate da Archiva, nell'erogazione dei propri servizi;
- le misure tecniche organizzative concordate fra Titolare e Archiva sono estese, laddove pertinente, agli eventuali ulteriori responsabili coinvolti nel trattamento;

Archiva S.r.l. Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR) T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com - Capitale sociale: euro 500.000,00 REA di VR: 319751 Iscritta Registro delle Imprese di Verona

- l'eventuale riuso di dispositivi di memorizzazione di massa avviene solo a seguito di cancellazione profonda del filesystem del supporto;
- Archiva tratta i dati personali dei Titolari, esclusivamente all'interno del territorio nazionale, presso la sede di Villafranca di Verona (VR).

Questo documento non può essere duplicato o diffuso senza l'esplicito consenso scritto di Archiva Group. Qualsiasi divulgazione, anche parziale, delle informazioni contenute nel presente documento che non sia stata preventivamente autorizzata da Archiva Group può costituire una violazione di legge. Per qualsiasi richiesta, si prega di contattare ciso@archivagroup.it