"IC" Outsourcing

Politica MG970 POL-12.15 POLITICA PER IL CLOUD

Funz. Emittente :	1000 – Direzione Generale		
Redatto da :	Roberto Coppola		
Verificato da :	Giulio Fanchin		
Approvato da:	Francesco Schinaia		
Versione	0	Data Versione:	08/03/2024
Descrizione modifiche			
Motivazioni	Prima emissione		
Collaborazioni :	Mattia Palesa		

Indice

Sommario

1 Introduzione al documento 3
1.1 Scopo e campo di applicazione del documento 3
1.2 Versione precedente 3
1.3 Livello di riservatezza 3
1.4 Riferimenti 3
1.5 Termini e definizioni 4

2 Missione 5
2.1 Definizione ed illustrazione dei ruoli e responsabilità 6

3. Individuazione logistica dei Server 7
3.1 Etichettatura delle Informazioni 7

4. Gestione degli Accessi 8
4.1 Limitazione degli Accessi 8

5. Crittografia 9

6. Change Management 10
6.1 Servizio di backup 10
6.2 Raccolta e Monitoraggio Log 10
6.3 Sincronizzazione degli orologi 10

7. Gestione delle Vulnerabilità e degli incidenti 11
7.1 Gestione degli Incidenti 11
7.2 Protezione delle Registrazioni 11
7.3 Audit Tecnici 11

8. Rimozione degli Asset 12

9. Monitoraggio del Cloud 13
9.1 Sicurezza delle Reti 13
9.2 Divulgazione delle Informazioni 13

10. Data Breach 14

11. Restituzione, Trasferimento e Smaltimento di dati personali 15
11.1 Accordi di Riservatezza 15

1 Introduzione al documento

Il presente documento, che è parte integrante del contratto di servizio fornito in modalità SaaS, redatto dalla IC Outsourcing (di seguito sempre definita solo come Organizzazione oppure ICO), descrive i requisiti specifici da soddisfare ed una dettagliata informativa al cliente sulle modalità di gestione delle attività in conformità a quanto previsto dalle linee guida ISO IEC 27017:2015 e ISO IEC 27018:2019.
L'Organizzazione fornisce servizi software in Cloud e in modalità SaaS. Per l'erogazione di detti servizi è utilizzato un provider certificato che garantisce ai clienti dell'Organizzazione la completa disponibilità dei loro dati e la necessaria ed assoluta Riservatezza, Integrità e Disponibilità degli stessi.

1.1 Scopo e campo di applicazione del documento

Il documento descrive il Sistema di Gestione IC Outsourcing conforme alle norme [ISO9001], [ISO 27001] e [ISO14001] [ISO27017] e [ISO27018] .

Il documento si applica alla Procedura [MG920] Procedura Integrata Qualità e Ambiente nell'ambito del Processo "Governance".

1.2 Versione precedente

Non presenti.

1.3 Livello di riservatezza

	Livello	Ambito di diffusione consentito
X	Pubblico	Il documento può essere diffuso **all'esterno** dell'azienda.
	Uso interno	Il documento può essere diffuso solo **all'interno** dell'azienda. Le terze parti a cui viene comunicato, hanno l'obbligo di non diffusione.
	Riservato	Il documento **non può essere diffuso** all'interno dell'azienda. La sua visibilità è limitata ad un gruppo ristretto di persone. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento .

1.4 Riferimenti

[ISO9001] norma UNI-EN-ISO 9001:2015 - "Sistema di Gestione per la Qualità"

[ISO27001] ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti): norma internazionale che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI

[ISO14001] norma UNI-EN-ISO 14001:2015 - "Sistema di Gestione per l'Ambiente"

[ISO27017] norma ISO/IEC 27017:2015 – "Controlli di Sicurezza per i Servizi Cloud"

[ISO27018] norma ISO/IEC 27018:2019 – "Standard di protezione dei dati per i Servizi Cloud"

[MG920] Procedura Manageriale MG920 Sistema Gestione Qualità

[PROCESSI] Insieme delle Procedure aziendali che permettono l'attivazione di Processi

1.5 Termini e definizioni

Vedi Glossario aziendale https://intranet.infocamere.it/web/intranet-ic-outsourcing/glossario
Di seguito i termini specifici di questo documento:

Termine	Descrizione
Cloud SaaS	Il Cloud SaaS, acronimo di Software as a Service, si riferisce a un modello di distribuzione software in cui le applicazioni sono ospitate da un provider di servizi cloud e messe a disposizione degli utenti via internet, eliminando la necessità di installazione e gestione locale da parte dell'utente.
Comitato Qualità	Comitato Indirizzo esteso al Responsabile Sistema Gestione Qualità e Servizi
Log	I log sono registri dettagliati di eventi, azioni o transazioni che si verificano all'interno di un sistema informatico. Questi registri contengono informazioni utili per il monitoraggio, la diagnosi dei problemi, l'analisi delle prestazioni e la sicurezza del sistema.
PII	PII sta per "Personally Identifiable Information", che in italiano significa "Informazioni personalmente identificabili". Si riferisce a qualsiasi informazione che può essere utilizzata per identificare in modo univoco, contattare o individuare una persona, come ad esempio nome, indirizzo, numero di telefono, indirizzo email, numero di previdenza sociale, numero di carta di credito e così via.
Sistema di Gestione	Sistema di Gestione integrata per la Qualità e l'Ambiente (SGQA)

2 Missione

IC Outsourcing Scrl si propone come un'Azienda leader nel guidare i propri clienti verso l'implementazione di soluzioni paperless, mediante la fornitura di soluzioni ICT e di consulenza specialistica per:

• la gestione e conservazione a norma dei documenti informatici;
• soluzioni trusted per attestare autenticità, integrità e valore legale dei documenti digitali;
• soluzioni per l'archiviazione documentale.

I nostri Clienti operano nella Pubblica Amministrazione. Il nostro interesse è quello di acquisire la loro fiducia in qualità di fornitori e di mantenere ed ampliare la nostra posizione di leader nel mercato digitale.

IC Outsourcing Scrl si impegna a comprendere le necessità dei clienti e pianificare le proprie attività per soddisfarle completamente attraverso l'identificazione e valutazione delle loro aspettative e la loro trasformazione in requisiti definiti e misurabili. Allo stesso modo opera nel rispetto delle richieste e dei requisiti:

• del mercato di riferimento;
• dello Stato in cui opera, adempiendo a leggi e regolamenti;
• di tutte le parti interessate.

Tali obiettivi sono raggiungibili da IC Outsourcing Scrl realizzando un Sistema di Gestione Integrato conforme alla norma UNI EN ISO 9001:2015 "Sistema Gestione Qualità", alla norma ISO/IEC 27001:2013 "Sistema Gestione Sicurezza delle Informazioni", alla norma ISO/IEC 27017:2015 "Controlli per la sicurezza delle informazioni dei servizi cloud", alla norma ISO/IEC 27018:2019 "Codice di condotta sulla protezione dei dati personali nel cloud" e in futuro alla norma UNI ISO 37001:2016 "Sistemi di Gestione per la Prevenzione della Corruzione".

IC Outsourcing assicura che vengano soddisfatte le seguenti condizioni:

• i dati archiviati sui server rimangono sempre di proprietà dell'Azienda;
• imporre adeguati controlli di accesso e garantire che i dati in transito e il caricamento o il trasferimento di file siano protetti con protocolli di crittografia;
• concedere la possibilità di scaricare una copia dei dati in qualsiasi momento ed in totale autonomia;
• monitorare periodicamente le prestazioni e il rispetto del contratto.

In tale ambito, il percorso definito dalla Direzione prevede:

• certificazione del Sistema di Gestione della Sicurezza delle Informazioni con estensione ai controlli delle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019 e mantenimento della stessa nel triennio successivo;
• rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il Rischio Residuo a livelli accettabili;
• attuazione, ove necessario, di idonee Azioni Correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
• definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (Business Continuity);
• stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

2.1 Definizione ed illustrazione dei ruoli e responsabilità

Per tutte le attività descritte la struttura funzionale e dirigenziale dell'Organizzazione fa capo alle figure di:

- Responsabile della Conservazione IC Outsourcing;
- Responsabile del Servizio di Conservazione a norma;
- Responsabile dello sviluppo e manutenzione del Sistema di Conservazione;
- Responsabile del Sistemi Informativi e della sicurezza di sistemi per la Conservazione;
- Responsabile per il Trattamento dati personali;
- Responsabile SGSI;
- Responsabile cybersecurity;

aventi responsabilità specifiche in materia di sicurezza delle informazioni. Inoltre il Responsabile Commerciale e il Responsabile tecnico dell'Area Corporate occupano il ruolo di interfaccia operativa tra l'Organizzazione e il cliente, in materia di sicurezza del cloud.
L'interfaccia principale è il Customer Care dell'Area Corporate ICO per quanto attiene le funzionalità del software fornito in modalità SaaS.
Il Responsabile del trattamento dei Dati (GDPR) ed il Designato al trattamento sono invece le funzioni preposte nell'Organizzazione per l'elaborazione dei dati personali (PII) prevista nei contratti; inoltre l'Organizzazione ha individuato al proprio interno - reparto Produzione - i punti di contatto con il cliente;
eventuali elaborazioni delle PII (ad esempio per motivi di assistenza e manutenzione), sono svolte dagli Autorizzati interni al trattamento.

3. Individuazione logistica dei Server

L'Organizzazione utilizza per i propri servizi in cloud infrastrutture all'interno del territorio nazionale italiano (Data Center del partner / fornitore InfoCamere Scpa ubicati a Padova e Milano) e piattaforma per la gestione di Conservazione a norma Ifin Sistemi Srl (Gruppo Zucchetti).
InfoCamere ScpA è certificata per i servizi di "Progettazione, realizzazione, erogazione e assistenza di servizi informatici per il trattamento sicuro e a conservazione di: informazioni, documenti informatici, identità digitali per le Camere di Commercio, le pubbliche Amministrazioni e terzi" secondo le norma ISO IEC 27001:2022 con estensione alle linee guida 27017:2015 e 27018:2019.
Ifin Sistemi Srl è certificata per i servizi di "Gestione della sicurezza delle informazioni per l'acquisizione ed il trattamento finalizzato alla conservazione e gestione dei dati e dei documenti informatici. Erogazione di servizi in modalità cloud SaaS" secondo le norma ISO IEC 27001:2013 con estensione alle linee guida 27017:2015 e 27018:2019.
L'Organizzazione, nell'eventualità di dover effettuare modifiche di change location sui servizi cloud attivati verso altri Data Center ubicati all'interno della UE, comunicherà tale variazione ai clienti con un preavviso di almeno 15 giorni, così come comunicherà per iscritto altre formalizzazioni che potranno riguardare eventuali espansioni infrastrutturali.

3.1 Etichettatura delle Informazioni

Laddove dai requisiti contrattuali o laddove si reputi necessario, l'Organizzazione rende noto al cliente le funzionalità dei servizi rivenduti su cloud che consentano un'adeguata etichettatura delle informazioni presenti sul cloud. Detta classificazione consente di regolamentare l'accesso alle sole funzioni che ne hanno l'autorità.

4. Gestione degli Accessi

L'Organizzazione regola la registrazione e de-registrazione all'applicazione e ai sistemi con modalità differenti a seconda dei servizi offerti.
Al Rappresentante del Cliente viene generata un'utenza "Avanzata" che individuerà una propria password.
L'utente Avanzato del Cliente avrà accesso alle principali funzioni del servizio Cloud.
L'utente registrato può provvedere alla richiesta di cancellazione (de-registrazione: si parla solo di cancellazione logica).
Per autenticare gli utenti l'Organizzazione assegna un codice di accesso, nome utente e password, e per questa sarà richiesta la modifica già al primo accesso.
L'Utente, avendo la possibilità di modificare autonomamente le password, consente in maniera tempestiva di intervenire nei casi di dubbi circa eventuali corruzioni o compromissioni di password, come i casi di divulgazioni involontarie.

4.1 Limitazione degli Accessi

Le limitazioni di accesso alle informazioni su cloud sono concordate in fase contrattuale con il Cliente.

5. Crittografia

Nel servizio cloud i flussi di dati da e verso i sistemi ed i server esposti su internet sono protetti mediante certificato SSL. L'Organizzazione mette in pratica una Privacy Policy descrivendo le modalità con cui tratta i dati personali nell'ambito della erogazione del servizio di Cloud Computing, anche alla luce degli obblighi imposti dal Regolamento UE 2016/679.
Relativamente allo Standard ISO/IEC 27018 ICO garantisce l'implementazione dei controlli richiesti per il trattamento di dati personali implementando adeguate misure di protezione, nel rispetto dei seguenti requisiti:
Scelta e Consenso: agevolazione dell'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'interessato, attraverso le indicazioni specificate nel contratto.
Finalità del trattamento: le finalità del trattamento sono rese note nel contratto di servizio.
Minimizzazione dei dati: file e documenti temporanei, nel caso in cui il sistema stesso non effettui la cancellazione automatica, sono cancellati o distrutti entro un periodo massimo di 6 mesi.
Limitazione all'uso, alla conservazione e alla divulgazione: Non avviene la divulgazione di dati personali a terze parti. La richiesta di divulgazione di dati personali da parte di autorità amministrative o giudiziarie è notificata al cliente in maniera tempestiva, ove consentito dalla legge.
Trasparenza: il ricorso a subappaltatori da parte del provider è reso noto al cliente del servizio Cloud prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto tra il provider e il cliente. Il provider informa il cliente in modo tempestivo di eventuali modifiche previste in questo senso.
Accountability: In caso di violazioni che comportano perdite, diffusione o modifica dei dati personali (data breach), effettua la notifica tempestivamente al cliente attraverso un processo interno di Incident Management.
Conformità alla privacy: il provider indica i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e indica specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Il provider informa tempestivamente il cliente di eventuali modifiche previste a tale riguardo.

6. Change Management

Per quanto attiene le eventuali modifiche al servizio cloud ed ai sistemi che lo compongono, l'Organizzazione provvederà tempestivamente a comunicarle ai clienti, fornendo i tempi di esecuzione delle variazioni così da minimizzare gli impatti che potrebbero derivare.

6.1 Servizio di backup

Il servizio di Backup è assicurato dal partner / fornitore InfoCamere. I tempi di conservazione sono definiti contrattualmente con il Cliente.

6.2 Raccolta e Monitoraggio Log

Le registrazioni dei log applicativi sono disponibili all'interno dell'Organizzazione, inoltre le modifiche alle informazioni personali vengono storicizzate e conservate, eventualmente anche a norma, con i log delle modifiche effettuate. Nel caso di contenziosi e/o richieste espresse dal Cliente, possono essere forniti.

6.3 Sincronizzazione degli orologi

L'Organizzazione per sincronizzare tutti gli orologi e mantenere coerenza degli eventi sul cloud si avvale del fornitore / partner InfoCamere che mette a disposizione un servizio di sincronizzazione temporale dei sistemi. Il servizio viene erogato da 3 time Server in alta affidabilità sincronizzati con la costellazione di satelliti GPS e galileo, tramite protocollo NTP.

7. Gestione delle Vulnerabilità e degli incidenti

L'Organizzazione predispone tutte le misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti. Sono definiti un team e delle risorse per eseguire periodiche e regolari scansioni di vulnerabilità e penetration test oltre a Audit di seconda parte.
L'Organizzazione esegue annualmente (o in caso di modifiche e/o richieste specifiche) test di vulnerabilità sugli applicativi; in caso di esiti negativi, provvede ad adottare le necessarie azioni correttive. Considerata la riservatezza di tali informazioni, l'esito dei test non è divulgato all'esterno.

7.1 Gestione degli Incidenti

L'Organizzazione ha definito una specifica procedura per poter permettere un approccio organizzato e regolato alla gestione degli incidenti come parte della propria strategia di sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.
Ogni segnalazione di evento che possa generare una compromissione deve essere segnalato al Dipartimento ICT (amministratori di Sistema) mediante mail dedicata amministratori.sistema@icoutsourcing.it riportando tutti gli elementi utili alla valutazione dell'evento. Tutte le segnalazioni pervenute saranno gestite da apposito team che valuterà se classificarle come incidente relativo alla sicurezza delle informazioni, rispondendo coerentemente a quanto previsto dalla procedura interna.
È a cura del Cliente sensibilizzare i propri dipendenti affinché forniscano informazioni relative al tipo di dati, alle informazioni, alla data e ora in cui si è verificato l'incidente e la posizione logica dei dati.
Se l'incidente di sicurezza delle informazioni è in relazione alle informazioni personali il Responsabile del Trattamento dei dati, oltre alle figure sopra richiamate, deve essere informato.
Il livello di impatto di un incidente di sicurezza delle informazioni sarà determinato secondo la strategia di gestione del rischio stabilita da RSGSI, con il Titolare del Trattamento ed il Responsabile del Sistemi Informativi e della sicurezza di sistemi per la Conservazione.
Il RSGSI manterrà una copertura del processo di gestione degli incidenti in relazione ad identificazione, valutazione, gestione e monitoraggio degli incidenti di sicurezza delle informazioni, compresa la raccolta di qualsiasi prova che potrebbe essere richiesta per l'analisi come prova forense.

7.2 Protezione delle Registrazioni

L'Organizzazione gestisce le registrazioni dei dati dei clienti (database) applicando le prassi di sicurezza previste dalle policies vigenti (https, cifratura del canale, ecc.). Inoltre, per la validazione delle soluzioni implementate, l'Organizzazione esegue con regolarità test di vulnerabilità.

7.3 Audit Tecnici

L'Organizzazione, avendo un sistema di gestione conforme alla ISO IEC 27001 e alle linee guida 27017-27018 esegue regolarmente Audit tecnici.

8. Rimozione degli Asset

Alla chiusura di un contratto con l'Organizzazione la piattaforma ferma i servizi, salvo che per quei diritti e obbligazioni per cui è espressamente prevista la sopravvivenza alla scadenza o risoluzione del contratto fatto salvo inoltre, l'adempimento di ogni obbligazione di pagamento maturata prima della scadenza o in costanza della risoluzione del contratto, ma non esegue la cancellazione effettiva. Dopo 60 giorni dall'avvenuto fermo dei servizi, gli asset del cliente presenti sui sistemi vengono cancellati definitivamente e non possono più essere recuperati.
La cancellazione avviene attraverso specifici accordi tra l'Organizzazione ed il partner / fornitore InfoCamere.
Nel caso in cui dovesse cessare il servizio di conservazione a norma erogato dall'Organizzazione, l'organizzazione stessa attiverà il piano di cessazione comunicato in fase di iscrizione al marketplace AgID.

9. Monitoraggio del Cloud

L'Organizzazione effettua il monitoraggio dei servizi cloud con gli strumenti messi a disposizione da InfoCamere; eventuali parametri di monitoraggio stabiliti in fase contrattuale saranno forniti a cura del Responsabile del Sistemi Informativi e della sicurezza di sistemi per la Conservazione.

9.1 Sicurezza delle Reti

Le reti virtuali sono definite dall'Organizzazione in base ai contratti stipulati con il partner / fornitore InfoCamere. I requisiti di configurazione sono definiti in funzione dei parametri di sicurezza desiderati.

9.2 Divulgazione delle Informazioni

A meno che non sia necessaria per soddisfare requisiti contrattuali non è prevista alcuna divulgazione di PII. L'eventuale divulgazione può avvenire solo verso dipendenti, fornitori o subappaltatori. In questi due ultimi casi l'Organizzazione richiede un espresso consenso da parte del Cliente, con esclusione di richieste legalmente vincolanti da parte delle autorità preposte (es. Autorità Giudiziaria).
Nei casi in cui avvenga un incidente che causa la divulgazione delle PII (es. data breach), la notifica al Responsabile Trattamento Dati sarà segnalata prima possibile, telefonicamente o di persona.
Qualsiasi divulgazione di PII deve essere registrata dal Responsabile Trattamento Dati nel registro di divulgazione delle PII. Tale documento deve comprendere quali informazioni personali sono state divulgate, da chi, a chi e a che ora.
Nei casi in cui la divulgazione è richiesta da autorità preposte, il riferimento legale utilizzato per autorizzare la divulgazione deve essere incluso nella registrazione.

10. Data Breach

È previsto l'intervento del Responsabile Trattamento Dati per la gestione del Data Breach in caso di eventi tracciabili di accesso non autorizzato alle PII o accesso non autorizzato alle apparecchiature o alle strutture di elaborazione che comportano perdita, divulgazione o alterazione delle PII.

11. Restituzione, Trasferimento e Smaltimento di dati personali

Il Responsabile Trattamento Dati dell'Organizzazione, deve garantire che la conservazione delle PII avvenga solo per il tempo necessario al raggiungimento delle finalità contrattuali.
Per quanto riguarda l'acquisizione, lo sviluppo e la manutenzione dei sistemi informativi, devono essere stabiliti requisiti per garantire che i file e i documenti creati nel normale corso delle operazioni, elaborazioni, vengano eliminati non appena tali file e documenti non siano più necessari. Le PII detenute eventualmente in formato cartaceo sono distrutte mediante il distruggidocumenti presente in azienda.

11.1 Accordi di Riservatezza

L'Organizzazione ha definito al proprio interno appositi accordi di riservatezza con il personale che opera in qualità di Autorizzato al trattamento sui servizi in Cloud forniti al cliente. Di norma non si producono stampe cartacee di materiali contenenti PII, eventuali stampe sono distrutte immediatamente dopo l'utilizzo. Gli interventi di assistenza, eseguiti su richiesta del cliente sono tracciabili mediante richieste dai Clienti (la piattaforma di ticketing) e non danno luogo ad archiviazioni di dati personali.
Le e-mail utilizzate dall'Organizzazione viaggiano su canale crittografato sia in ingresso che in uscita, garantendo in tal modo che eventuali dati personali trasmessi (sebbene la policy aziendale vieti la trasmissione di PII mediante e-mail) lo facciano in modo sicuro.
Laddove l'organizzazione operi su PII del cliente, richiede formalmente una nomina a Autorizzato al trattamento, coperta dai vincoli di cui al regolamento 2016/679.
InfoCamere non fa uso di subappaltatori per l'elaborazione dei dati.