AFFIDAMENTO DEI SERVIZI CLOUD

1. PREMESSA

L'affidamento dei dati in cloud ai sensi della ISO 27017:2015 prevede la verifica di determinati requisiti sia per il Cliente che per ACCA software S.p.a..

ACCA software S.p.a. in completa trasparenza per la gestione dei servizi offerti fornisce in seguito un riepilogo degli adempimenti riferiti al Cliente a quelli adottati da ACCA software S.p.A. come fornitore in ottemperanza alla ISO 27017: 2015.

Qualora riscontriate delle difformità rispetto a quanto sotto riportato e gli eventuali servizi offerti, vi invitiamo a segnalarcelo tramite i nostri consueti canali di comunicazione.

2. PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte di ACCA software S.p.A.; a tutela del Cliente, ACCA software S.p.A. adotta metodi e processi certificati da terziin ambito ISO 27001, ISO 27017 e ISO 27018;

1. ACCA software S.p.A. ha identificato nel Garante della Privacy, Agid e nella Polizia Postale le Autorità rilevanti per la protezione dei dati.
   Qualora il Cliente ritiene di modificare e/o integrare tali organismi, è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.
   Si ricorda che il Cliente è tenuto ad aggiungere ai propri programmi di formazione iseguenti elementi di sensibilizzazione, istruzione per:
   - i responsabili di funzione;
   - i referenti di funzione (sys admin, security admin etc.);
   - gli utenti del servizio cloud, inclusi i dipendenti e gli appaltatori interessati.

   La consapevolezza della sicurezza delle informazioni, i programmi di istruzione e formazione sui servizi cloud dovrebbero essere formalizzati alla direzione ed ai responsabili della supervisione, compresi quelli delle unità operative.

   Questi sforzi supportano un efficace coordinamento delle attività di sicurezza delle informazioni in ambiti quali:

- standard e procedure per l'utilizzo dei servizi cloud;
- rischi per la sicurezza delle informazioni relativi ai servizi cloud e come tali rischisono gestiti;
- rischi per l'ambiente di rete e di sistema con l'uso di servizi cloud;
- considerazioni legali e normative applicabili.

2. ACCA software S.p.A. eroga i propri servizi cloud su infrastrutture residenti all'interno della Comunità Economica Europea e specificatamente presso i Data Center ubicati nelle Region AWS denominate Europa (Irlanda eu-west-1) ed Europa (Francoforte eu-central-1).

3. ACCA software S.p.A. comunicherà al Cliente con un preavviso di 15 giorni eventuali impatti e/o modifiche di change location sui servizi cloud attivati verso altri Data Center Amazon Web Services ubicati all'interno della UE ed il rispetto del trattamento dei dati conforme alla direttiva europea sulla protezione dei dati (GDPR. 679/2016).
4. ACCA software S.p.A. classifica tutte le informazioni scambiate con il Cliente, l'etichettatura segue vari livelli di classificazione:
5. L'inventario delle risorse che effettua periodicamente ACCA software S.p.A. tiene conto delle informazionie delle risorse associate e archiviate nell'ambiente di cloud computing. I registri dell'inventario indicano dove vengono mantenute le risorse.
6. Ogni informazione dislocata nel cloud di ACCA software S.p.A. è identificata ed etichettata. Una apposita procedura interna ne garantisce l'applicazione.
7. ACCA software S.p.A. adotta un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e conferma che è nelle condizioni di adempiere ai propri ruoli e responsabilità in materia di sicurezza dei dati.
   A tal fine, sono condotte periodiche rivalutazioni dell'analisi dei rischi, vulnerability assessment e penetration test.
   Il Cliente che ritiene di modificare e/o integrare le prassi di controllo di ACCA software S.p.A. è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.
   ACCA software S.p.A. rimane a completa disposizione del Cliente sia per fornirgli il registro del trattamento dei servizi in essere sia per dargli indicazioni circa la procedura di classificazione delle informazioni attraverso il proprio sito web – https://www.acca.it
8. Il Cliente deve richiedere informazioni a ACCA software S.p.A. sulla gestione delle vulnerabilità tecniche che possono influenzare i servizi forniti. In ogni caso, in tale ambito ACCA software S.p.A. adotta una propria politica di vulnerability assessment e di penetration test; su esplicita richiesta del Cliente, ACCA software S.p.A. è in grado di fornire documentazione a riguardo.
9. Tutti gli accessi ai sistemi di informazione di ACCA software S.p.A. devono avvenire in modo sicuro e protetto.
10. Il Cliente deve sempre utilizzare tecniche di autenticazione sufficienti per autenticare i suoi utenti con profilo amministratore (ma anche user); a tale scopo, opportune policy adottate da ACCA software S.p.A. impediscono di usare credenziali deboli o inadatte allo scopo.
11. Il Cliente è tenuto a verificare e garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate includendo:
    - la limitazione dell'accesso ai servizi cloud;
    - alle funzioni del servizio cloud;
    - ai dati dei clienti gestiti dal servizio cloud.
12. Il processo di gestione del servizio in cloud offerto al Cliente tiene conto del profilo di accesso al servizio fornito da ACCA software S.p.A. che provvede ad informare il Cliente sulle modalità diaccesso standard, durante l'attivazione del servizio.
13. Per fruire del servizio cloud devono essere ben definiti gli utenti.A tal fine, ACCA software S.p.A. adotta due diversi profili ad uso del Cliente:
    - Customer User as Administrator - amministratori del servizio cloud che hanno accesso privilegiato;
    - Customer User - Utenti con un profilo User, che possono eseguire operazioni limitate.
14. il Cliente è tenuto a verificare che la procedura di gestione di ACCA software S.p.A. per l'allocazione delle informazioni di autenticazione segreta, come le password, soddisfi i propri requisiti.
15. ACCA software S.p.A. adotta una specifica procedura scritta per il controllo e la manutenzione dell'efficacia delle chiavi crittografiche per ciascuna fase del ciclo di vita, ossia: la generazione, la modifica o l'aggiornamento, la memorizzazione, il ritiro, il recupero, il mantenimento e ladistruzione. Normalmente

ACCA software S.p.A. applica i controlli crittografici su tutte le transazionida/per il Cliente, con standard di protezione in linea con il mercato, con valutazione periodica dello stato del certificato utilizzato.

E' compito del Cliente esaminare tutte le informazioni fornite da ACCA software S.p.A. per confermare se le funzionalità di crittografia:

- soddisfano i suoi requisiti di politica;
- sono compatibili con qualsiasi altra protezione crittografica già utilizzata;
- sono applicate ai dati a riposo ed in transito e all'interno del servizio.

16. ACCA software S.p.A. ha specifiche politiche e procedure scritte per lo smaltimento sicuro o il riutilizzo delle risorse. Se richiesto, ACCA software S.p.A. fornirà tali documenti.
17. Tutti i tentativi di log-on errati, vengono registrati. Superati i trenta tentativi di accessi errati l'accesso ai servizi viene bloccato per 15 minuti, i successivi tentativi potranno essere effettuati al più una volta per minuto per 12 ore.
18. Le password non sono mai registrate in chiaro.
19. Le chiavi di accesso non possono essere condivise e devono essere uniche per ciascun utente.
20. Le chiavi di accesso non devono essere tenute su supporti scritti con indicazioni che possono facilitare l'accesso non autorizzato da parte di terzi.
21. ACCA software S.p.A. fornisce funzionalità automatiche di backup e disaster recovery per i servizi cloud erogati ai propri clienti.
22. Ogni dodici mesi ACCA sottopone a test i propri backup verificandone il buono stato in modo da ottenere dei ripristini sicuri e non compromessi.
23. Tutte le attività rivolte alla risoluzione di problematiche di sicurezza e/o fruibilità dei servizi cloud saranno svolte da personale ACCA software S.p.A. con opportuni permessi e deleghe. Gli accessi saranno registrati con timestamp e certificati da audit esterni. Le attività saranno strettamente correlate alla risoluzione del problema nel rispetto dei criteri di integrità, riservatezza, disponibilità ed autenticità.
24. Laddove richiesto ciascun operatore che svolge attività in esterna potrà collegarsi alle Facilities tramite l'instaurazione di un collegamento virtuale VPN (Virtual Private Network) punto-punto tra l'operatore – client - ed il *site* di destinazione seguendo un percorso definito e segregato per l'accesso al target.
25. ACCA software S.p.A. adotta una policy di sincronizzazione di tutti gli orologi aziendali, e ne verifica periodicamente l'applicazione, in modo da garantire che ogni ambiente sia sincronizzato.
26. ACCA software S.p.A. adotta una politica di segregazione delle reti per ottenere l'isolamento nell'ambiente condiviso per il servizio cloud. Su esplicita richiesta del Cliente, ACCA software S.p.A. è in grado di fornire documentazione a riguardo.
27. Il Cliente deve determinare i requisiti di sicurezza delle informazioni e quindi valutare se iservizi offerti da ACCA software S.p.A. soddisfino tali requisiti. Per questa valutazione, il Cliente può semprerichiedere a ACCA software S.p.A. informazioni sulle funzionalità di sicurezza delle informazioni adottate.
28. ACCA software S.p.A. effettua le operazioni di sviluppo in ambiente sicuro e dedicato, con dati di prova non reali. Le operazioni di sviluppo sono governate da specifiche procedure scritte. Su esplicita richiesta del Cliente, ACCA software S.p.A. è in grado di fornire documentazione a riguardo.
29. Il Cliente deve includere ACCA software S.p.A. nella sua politica di sicurezza delle informazioni, nelle relazioni con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati gestiti nei servizi offerti da ACCA software S.p.A..
30. ACCA software S.p.A. ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni.

    Questa policy, serve per assicurare un approccio coerente ed efficace per la gestione degli incidenti alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.

    La politica mira a mitigare i seguenti rischi:

    - ridurre l'impatto delle violazioni della sicurezza delle informazioni garantendo chegli incidenti siano seguiti correttamente.

- aiutare ad identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti, diminuendo la superficie di attacco e le possibilità di Data Breach.

Gli incidenti di sicurezza delle informazioni devono essere segnalati il più presto possibile inviando un'email a cybersec@acca.it verificata la comunicazione da parte del personale preposto si riunirà in misura straordinaria l'Incident Response Team che delibererà sulle opportune azionicorrettive e/o blocco.

In caso di "Data Breach", devono essere segnalati al DPO che provvede ad inoltrarli all'Autorità di Controllo dei Dati Personali, il "Garante", nei mezzi che il Garante renderà noti.

La definizione di un "incidente di sicurezza delle informazioni" è un evento avverso che ha causato o ha il potenziale di causare danni al patrimonio, alla reputazione, ai Clienti e/o al personale della ACCA software S.p.A., nei termini che gli attacchi o gli incidenti possono essere indirizzati o occorre anche ai Sistemi di Elaborazione che erogano i Servizi di cui usufruiscela ACCA software S.p.A. stessa.

Un incidente di sicurezza delle informazioni include, ma non è limitato a, quanto segue:

- la perdita o il furto di dati o informazioni (Data Loss);
- il trasferimento di dati o informazioni a coloro che non hanno diritto a ricevere quell'informazione (Data Leakage);
- tentativi (falliti o riusciti) di ottenere accesso non autorizzato ai dati o archivi (DataStore) delle informazioni di un sistema informatico dell'Organizzazione o dei Suoi Clienti;
- modifiche alle informazioni o ai dati o all'hardware del sistema, firmware o software senza autorizzazione e/o senza che il RSGSI o la Direzione ne siano a conoscenza e senza l'istruzione o il consenso di RSGSI e della Direzione;
- Interruzione indesiderata di un servizio erogato dai Sistemi dell'Organizzazione;
- l'uso non autorizzato di un sistema per l'elaborazione o l'archiviazione di dati da parte di qualsiasi persona interna o esterna all'organizzazione;
- l'azione di un malware o un attacco DDOS.

E' vitale quindi che il Cliente ed i collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.

Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.

Sarà cura di ACCA software S.p.A. rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.

La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri.

L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.

In prima istanza l'analisi degli incidenti spetta al SOC e in caso di particolari difficoltà al SOC Supervisor e al RSGSI.

Se l'incidente di sicurezza delle informazioni è in relazione alle informazioni personali, sia su formato cartaceo che elettronico, il responsabile della protezione dei dati (DPO), 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 SOC Supervisor sentita il Data Subject ed il DPO. Di tali incontri e indirizzi strategici andrà redatto un apposito documento, che verrà aggiornato ad ogni audit.

Degli incidenti di sicurezza delle Informazioni, andrà redatto un Registro "Incident Report" e tale elenco farà parte del riesame annuale e degli Audit Infrannuali.

La gestione degli incidenti riguarda l'intrusione, il compromesso e l'abuso di informazioni e risorse informative e la continuità delle informazioni critiche relative a sistemi e processi.

Il responsabile dei servizi IT (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 prove forensi.

I servizi IT di ACCA software S.p.A. garantiranno che solo il personale identificato e autorizzato abbia accesso ai sistemi interessati durante l'incidente e che tutte le azioni correttive siano documentate nel modo più dettagliato possibile.

La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni, deve essere utilizzata per ridurre la verosimiglianza o l'impatto di incidenti futuri.

I Responsabili ICT esamineranno regolarmente gli incidenti di sicurezza delle informazioni effettuando ex Post una revisione dell'incidente.

I tipi ed i volumi di incidenti e costi sostenuti durante il verificarsi degli incidenti saranno analizzati per identificare eventuali modelli o tendenze (al ribasso o al rialzo).

In caso di tendenza al rialzo, le contromisure di sicurezza andranno ovviamente riviste (Riesame).

Il responsabile dei servizi IT (RSGSI) condividerà questa analisi, se del caso, con il "Reporting Point" designato (SOC Supervisor o NOC Supervisor) per aiutare il processo automatico di allerta per l'Organizzazione e stabilire dei meccanismi di Warning e Critical in linea con le esigenze riscontrate per un intervento migliore e più tempestivo.

31. Tutti i dati gestiti in transito o meno sono crittografati dalla ACCA software S.p.A.. Per i dati in transito, viene utilizzata la crittografia TLS 1.2 o versione successiva. In caso contrario, viene utilizzata la crittografia AES 256 o versione successiva.
32. Il Cliente deve considerare che Leggi e Regolamenti pertinenti possono essere quelli delle giurisdizioni che regolano ACCA software S.p.A., oltre a quelli che regolano lui stesso.
33. Il Cliente deve richiedere evidenza della conformità di ACCA software S.p.A. con le normative e gli standard pertinenti richiesti per le sue attività. Tali prove possono essere le certificazioni prodotte dagli auditor di terze parti in ambito ISO o modelli di gestione esposte nel sito https://www.acca.it .
34. In caso di forza grave - calamità naturali, eventi terroristici ovvero ogni fatto catastrofico, ragionevolmente imprevedibile, conseguente a eventi determinanti, e a loro volta ragionevolmente imprevedibili alle strutture deposte all'erogazione dei servizi Cloud dei clienti, se prevista sottoscrizione Disaster Recovery questi verranno migrati in altro DC specificato in fase contrattuale.
35. Si ricorda che il Cliente deve definire o estendere le sue politiche e procedure esistenti in conformità con il suo uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso del servizio cloud.
36. I dati archiviati sui server della ACCA software S.p.A. saranno sempre di proprietà del Cliente.
37. ACCA software S.p.A. concede la possibilità di scaricare una copia dei dati in qualsiasi momento ed in totale autonomia e dichiarare con la massima trasparenza il luogo fisico dove risiedono i dati.
38. ACCA facilita la portabilità nel caso in cui il cliente decidesse di migrare applicazioni e dati da un ambiente cloud ad un altro evitando di rimanere 'bloccati' (vendor lock-in).

39. Si ricorda che il Cliente deve richiedere a ACCA software S.p.A. una descrizione documentata del processo di cessazione del servizio che copra la rimozione delle risorse del Cliente seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi di ACCA software S.p.A.. A tal fine, ACCA software S.p.A. ha una specifica procedura scritta per la dismissione del servizio, ivi inclusa la modalità di restituzione dei dati (ove necessario).
40. Schema e principali allegati di un contratto di Servizi di cloud computing della ACCA software S.p.A.:
    - Premesse e Definizioni;
    - Oggetto e Finalità;
    - Specificazioni Tecniche del servizio affidate a uno o più allegati;
    - Modalità di perfezionamento del contratto;
    - Livelli e Modalità di mantenimento del servizio e assistenza;
    - Corrispettivi (pay for use o canoni per servizi differenziati);
    - Responsabilità fornitore e Responsabilità Cliente (eventuale possibilità di sospensione del servizio);
    - Recesso e risoluzione (con clausola risolutiva espressa);
    - Obblighi di riservatezza (anche successivi alla conclusione del contratto);
    - Proprietà e licenze delle prestazioni oggetto del contratto (software anche di terzi, domain name, loghi etc.);
    - Fase patologica (controversie, fallimento del Fornitore del servizio e del Cliente etc.);
    - Modalità delle comunicazioni e protezione dei dati;
    - Modifiche del contratto e Cessione del contratto;
    - Durata del contratto;
    - Legge applicabile e Giudice Competente (o Arbitro);
    - SLA [livelli di servizio su accessibilità alla piattaforma, livelli di servizio su modalità di ripristino, livelli di servizio su tempistiche di assistenza (e risoluzione) in caso di problemi di utilizzo, livelli di utilizzabilità della piattaforma e verifica di eventuali rallentamenti nella fornitura del servizio, livelli di servizio sul mantenimento dei dati (e documenti) etc.] e penali (ed eventuali delimitazioni dell'indennizzo).
    - Ammissibilità anche in caso di colpa grave o violazione di misure di sicurezza minime, necessarie o idonee);
    - Policy di utilizzo della piattaforma;
    - Privacy Policy con nomina in capo al cloud provider come Responsabile del trattamento;
    - Data Privacy Officer – privacy@acca.it;
    - Definizione di misure di sicurezza a presidio della piattaforma (definizione di politiche di prevenzione da accessi abusivi con definizione di tecniche funzionali al controllo degli accessi e di verifica dell'integrità dei dati e di monitoraggio/reporting in caso di accessi abusivi con eventuale perdita parziale del dato);
    - Specificazioni Tecniche su soluzioni fornite e tecnologia utilizzata;
    - Eventuali certificazioni ottenute.
41. ACCA software S.p.A. si impegna affinché tutte le informazioni, concetti, idee, procedimenti, metodi e/o dati tecnici di cui il personale utilizzato dal medesimo verrà a conoscenza nello svolgimento del servizio sono considerati riservati e coperti da segreto.

    ACCA software S.p.A. infine accetta di non divulgare, comunicare o diffondere i dati dallo stesso acquisiti in ragione della attività di cui alla presente procedura, né altrimenti utilizzarli per la promozione e la commercializzazione dei propri servizi.

    ACCA software S.p.A. si obbliga ad adottare con i propri dipendenti e consulenti tutte le cautele necessarie a tutelare la riservatezza di tali informazioni e/o documentazione ed a sottoscrivere, in fase di avvio dei servizi, apposito accordo di riservatezza.

ACCA software S.p.A. ottempera la normativa in materia di trattamento dei dati personali nonché i diritti delle persone fisiche e degli altri soggetti secondo quanto stabilito dal Codice di protezione dei dati personali (D.lgs. 196/03 e s.m.i. e Regolamento 2016/679 e sue applicazioni).

42. La cessazione dei servizi cloud segue un flusso suddiviso in n.5 stati.
    i. Ricezione a mezzo PEC della richiesta di cessazione del/dei servizio/servizi da parte del Cliente
    ii. Verifica stato del Cliente e durata contrattuale
    iii. Verifiche Tecniche
    iv. Cessazione servizio/servizi
    v. Invio comunicazione a mezzo PEC al Cliente dell'avvenuta cessazione.

    A seconda della specifica finalità del trattamento, i tempi di conservazione sono fissati dalla legge (24 mesi ad esempio per la conservazione dei tabulati telefonici).

    ACCA software S.p.A. ottempera al diritto all'oblio di cui all'art. 17 del GDPR è il diritto alla cancellazione dei dati di una persona fisica, esteso e regolato anche con riferimento alla società digitale.

    Il diritto alla cancellazione prevale quindi sull'interesse alla conservazione: nei casi previsti, se un interessato chiede la cancellazione dei propri dati ACCA software S.p.A. procederà senza ingiustificato ritardo, e quindi senza riservarsi di continuare a trattare il dato sino alla scadenza originariamente fissata, prossima o meno che sia.
43. ACCA software S.p.A. adotta l'hardening, cioè il rafforzamento delle piattaforme installate dal punto di vista della security.
44. Tutte le comunicazioni erogate da ACCA software S.p.A. avvengono tramite protocollo HTTPS, SSL e TLS garantendo che i dati trasmessi raggiungano la corretta destinazione.
45. ACCA software S.p.A. registra i log di tutti i restore dei backup su appositi repository.
46. ACCA software S.p.A. assicura un uso limitato del materiale cartaceo. Il materiale a sua volta viene distrutto attraverso la triturazione degli stessi.
47. ACCA software S.p.A. assicura il mantenimento delle copie delle politiche di sicurezza e delle procedure operative per un periodo di 12 mesi.