

Protocollo affidamento servizi cloud

Economics Living Lab

INDICE DELLE REVISIONI					
Versione	Data	Oggetto	Redatto	Verificato	Approvato
1.0	29/07/2025	Prima emissione	COM	DIR	DIR

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

Premessa

L'affidamento dei dati in cloud prevede la verifica di determinati requisiti sia per il Cliente che per Economics Living Lab.

Economics Living Lab in completa trasparenza per la gestione dei servizi offerti Vi fornisce di seguito un riepilogo dei Vostri adempimenti anche riferiti a quelli che Economics Living Lab adotta come fornitore in ottemperanza alla ISO 27017:2015.

Qualora riscontriate delle difformità rispetto a quanto sotto riportato e agli eventuali servizi offerti Vi invitiamo a segnalarcelo prontamente.

Politica per la sicurezza delle informazioni

Economics Living Lab ha deciso di adottare un sistema di gestione integrato relativamente alle norme:

- UNI EN ISO 9001:2015 relativa al sistema di gestione della qualità
- ISO/IEC 27001:2022 relativa al sistema di gestione della sicurezza delle informazioni
- ISO/IEC 27017:2015 relativa alla gestione della sicurezza nel cloud computing
- ISO/IEC 27018:2019 relativa alla gestione della sicurezza delle informazioni in cloud

Il sistema di gestione integrato di Economics Living Lab è strutturato in modo da garantire la sicurezza delle informazioni (riservatezza, integrità e disponibilità dei dati) nel rispetto delle suddette norme.

Economics Living Lab, inoltre, si impegna nel raggiungimento della conformità normativa rispetto alla legislazione applicabile in materia di protezione dei dati personali.

Economics Living Lab ha redatto, approvato e pubblicato la Politica del Sistema di Gestione Integrato, rendendola disponibile sul proprio sito internet istituzionale, al fine di garantirne la diffusione e la trasparenza verso tutte le parti interessate.

Ruoli e responsabilità

Economics Living Lab ha definito in modo chiaro e documentato i ruoli e le responsabilità all'interno della propria Organizzazione, con particolare attenzione alla gestione dell'ambiente cloud. Tali responsabilità includono la supervisione della sicurezza delle informazioni, la gestione operativa dei servizi cloud, la conformità normativa e contrattuale, nonché la continuità operativa.

Nello specifico, per le attività sopra descritte le figure preposte sono quelle di Responsabile del Sistema di Gestione Integrato (RSGI) e di Amministratore di Sistema (AdS).

Il Titolare del trattamento (GDPR) e l'amministratore di sistema sono le funzioni preposte da Economics Living Lab per l'elaborazione dei dati personali prevista nel contratto. Eventuali elaborazioni dei dati personali connesse alle attività istituzionali dell'Organizzazione sono svolte da personale interno, opportunamente designato e formato in materia di protezione dei dati personali.

Il punto di contatto per qualsiasi riferimento ad eventi e/o incidenti di sicurezza è: info@econlivlab.eu.

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

GESTIONE DEI DATI IN CLOUD

1.1. I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte di Economics Living Lab; a tutela del Cliente Economics Living Lab adotta l'applicazione di metodi e processi certificati da terzi in ambito ISO 27001, ISO 27017, ISO 27018;

1.2. Economics Living Lab utilizza per i propri servizi in cloud infrastrutture situate all'interno del territorio nazionale italiano e/o europeo; i fornitori dell'infrastruttura cloud sono opportunamente selezionati e qualificati nonché certificati secondo le norme ISO/IEC 27001:2022 con estensione alle linee guida ISO 27017:2015 e ISO 27018:2019;

1.3. Qualora Economics Living Lab dovesse effettuare modifiche nella localizzazione dei servizi cloud attivati verso altri datacenter comunicherà tale variazione ai clienti con un preavviso di almeno 15 giorni; tale modalità comunicativa verrà utilizzata anche nel riguardo di altre modifiche infrastrutturali sostanziali;

1.4. Per usufruire del servizio cloud Economics Living Lab ricorda al Cliente che sono ben definiti i profili utente. A tal fine Economics Living Lab adotta due diversi tipologie di profili:

- utenti del Cliente con profilo amministratori del servizio cloud che hanno accesso privilegiato;
- utenti con un profilo User, che possono eseguire operazioni limitate.

1.5. Come indicato in premessa, Economics Living Lab ha stabilito 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, conduce periodiche rivalutazioni dell'analisi dei rischi, test di vulnerabilità e di penetrazione dei sistemi. Il Cliente che ritiene di modificare e/o integrare le prassi di controllo di Economics Living Lab è tenuto a definire tali aspetti preventivamente in uno specifico accordo tra le parti.

1.6. Economics Living Lab identificato nel Garante della Privacy, Agid e nella Polizia Postale, le Autorità rilevanti per la protezione dei dati. Qualora il Cliente ritenesse di modificare e/o integrare tali organismi, è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti. Salvo espressamente vietato dalla legge, se una Autorità Giudiziaria dovesse richiedere dati o informazioni del Cliente a Economics Living Lab, quest'ultima si impegna a dare comunicazione al Cliente circa i dati e le informazioni comunicate, mediante indirizzo PEC ufficiale del Cliente.

1.7. Si ricorda che il Cliente è tenuto ad aggiungere ai propri programmi di formazione i seguenti elementi di sensibilizzazione, istruzione per le figure che direttamente hanno accesso ai servizi cloud quali: i responsabili, gli amministratori, gli integratori di servizi cloud, 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 forniti alla direzione ai responsabili della supervisione, compresi quelli delle eventuali unità operative presenti. 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 relative ai servizi cloud e come tali rischi sono gestiti, rischi per l'ambiente di rete e di sistema con l'uso dei servizi cloud, considerazioni legali e normative applicabili.

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

1.8. L'inventario delle proprie risorse che effettua periodicamente Economics Living Lab tiene conto delle informazioni e delle risorse associate e archiviate nell'ambiente di cloud computing. I registri dell'inventario indicano dove vengono mantenute le risorse.

1.9. Economics Living Lab colloca i dati dei clienti sempre e solo su server all'interno dell'Unione Europea.

1.10. Ogni informazione dislocata nel cloud di Economics Living Lab è identificata ed etichettata. Economics Living Lab ha provveduto a redigere una procedura interna che ne garantisca l'effettiva applicazione. Detta classificazione consente di regolamentare l'accesso alle informazioni alle sole funzioni che ne hanno l'Autorità sulla base dell'etichettatura stessa.

1.11. Economics Living Lab rimane a completa disposizione del Cliente sia per fornire l'eventuale registro dei trattamenti per i servizi in essere come responsabile, sia per dare indicazione circa la procedura di classificazione dell'informazioni attuata, come disposto al precedente articolo.

1.12. La politica di controllo degli accessi in cloud al servizio che adotta Economics Living Lab prevede la compartimentalizzazione per ciascun servizio cloud.

1.13. Economics Living Lab, se non diversamente definito fra le parti, genera l'utenza di amministratore del Cliente che individuerà una propria password. Sarà l'utente amministratore a creare le utenze user del Cliente. Per ogni utenza user verrà generata automaticamente una password e per questa sarà richiesta all'utenza generata la modifica al primo accesso. L'utenza del Cliente potrà modificare in autonomia le password ma in caso di dubbi, corruzioni o compromissioni, come nei casi di divulgazione involontaria, ne darà comunicazione immediata ad Economics Living Lab attraverso la mail del punto di contatto

1.14. Si ricorda che il Cliente deve sempre utilizzare tecniche di autenticazione sufficienti per autenticare i profili di amministratore e di user a tal scopo Economics Living Lab adotta policy che impediscano di usare credenziali deboli o inadatte allo scopo; tuttavia, Economics Living Lab invita il Cliente a verificare che politiche di gestione delle informazioni di autenticazioni segrete soddisfino i requisiti del Cliente, in caso contrario tali aspetti saranno preventivamente definiti in uno specifico accordo tra le parti.

1.15. Economics Living Lab invita il Cliente a verificare e garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la propria politica di controllo degli accessi e che tali restrizioni siano realizzate. Ciò include: la limitazione dell'accesso ai servizi cloud, le funzioni e i dati gestiti all'interno del servizio stesso. In caso le limitazioni di accesso alle informazioni non siano sufficienti o in conformità alle politiche del Cliente, esso ne dovrà rendere nota ad Economics Living Lab e tali aspetti saranno definiti in uno specifico accordo tra le parti.

1.16. Laddove sia consentito l'utilizzo di programmi di utilità, il Cliente deve identificare tali programmi nel proprio ambiente e assicurarsi che non interferiscano con i controlli del servizio cloud.

1.17. Per l'utilizzo dei servizi cloud il Cliente, se giustificato dalla propria analisi del rischio, dovrà implementare adeguati controlli crittografici. Tali controlli dovranno essere sufficienti a mitigare i rischi identificati, indipendentemente dal fatto che tali controlli siano forniti da Economics Living Lab. Nei servizi cloud i flussi di dati da e verso i sistemi e di server esposti su Internet sono protetti utilizzando un canale sicuro TLS mediante opportuna configurazione. Economics Living Lab ricorda al Cliente di esaminare le informazioni fornite per confermare le funzionalità crittografiche e che esse soddisfino i requisiti delle

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

proprie politiche interne nonché che esse siano compatibili con qualsiasi altra protezione crittografica già in uso presso il Cliente. Economics Living Lab ricorda al Cliente che esso non dovrebbe consentirgli di archiviare e gestire le chiavi di crittografia per le operazioni crittografiche quando il Cliente impiega una sua propria gestione delle chiavi o un servizio di gestione delle chiavi separato e distinto. In tal caso il Cliente deve rendere noto ad Economics Living Lab in fase contrattuale tale evenienza.

1.18. Economics Living Lab adotta specifiche politiche per lo smaltimento sicuro o il riutilizzo delle risorse. Nel caso il Cliente ne chieda evidenza dovrà inviare regolare comunicazione al punto di contatto.

1.19. Per quanto attiene le eventuali modifiche al servizio cloud e ai sistemi che lo compongono, Economics Living Lab provvederà a tempesta tempestivamente a comunicarlo ai clienti, fornendo i tempi di esecuzione delle variazioni così da minimizzare gli impatti che potrebbero derivarne.

1.20. Il servizio di backup è assicurato da Economics Living Lab. Il Cliente, in sede contrattuale dovrà richiedere le specifiche delle capacità di backup applicate da Economics Living Lab nonché verificare che tali specifiche siano compatibili con le proprie necessità di conservazione. Qualora non sia Economics Living Lab a fornire il servizio di backup, ovvero quando sia stata contrattualizzata tale opzione, il Cliente si rende responsabile dell'implementazione del mantenimento e della verifica delle necessarie funzionalità di backup.

1.21. Economics Living Lab implementa un set di log standard che consentono di monitorare una serie di eventi. Ciò non toglie che il Cliente sia tenuto a verificare se tale impostazione sia sufficiente in linea con le proprie politiche; diversamente il Cliente dovrà definire con Economics Living Lab i requisiti per la registrazione degli eventi in separato accordo tra le parti.

1.22. Economics Living Lab per sincronizzare tutti gli orologi e mantenere coerenza degli eventi sul cloud utilizza il sistema NTP. Economics Living Lab verifica periodicamente che ogni ambiente sia sincronizzato.

1.23. Economics Living Lab ha predisposto le misure necessarie per ricercare, governare e risolvere le vulnerabilità tecniche individuate al fine di evitare e/o minimizzare impatti negativi sul servizio e sui dati gestiti. Tuttavia, Economics Living Lab ricorda al Cliente che la gestione operativa delle vulnerabilità tecniche relative ai prodotti e ai servizi sono in capo al Cliente stesso che dovrà definire un proprio processo di gestione.

1.24. Economics Living Lab adotta una politica di separazione delle reti per ottenere l'isolamento nell'ambiente condiviso per i servizi cloud. Su esplicita richiesta del Cliente Economics Living Lab è in grado di fornire documentazione a riguardo

1.25. il Cliente dovrà valutare se il servizio offerto da Economics Living Lab soddisfa i propri requisiti di sicurezza dell'informazione. A tal fine il Cliente può sempre richiedere ad Economics Living Lab informazioni sulle funzionalità di sicurezza delle informazioni adottate.

1.26. Economics Living Lab 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 che possono essere fornite al Cliente, sulla base di richiesta esplicita scritta.

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

1.27. Il Cliente dovrà includere Economics Living Lab 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 nel servizio offerti da Economics Living Lab.

1.28. Il Cliente deve confermare i ruoli e le responsabilità in materia di sicurezza delle informazioni relative al servizio cloud, descritti nel contratto. Questi possono includere a seconda dei servizi offerti i processi quali: protezione da malware, backup, controlli crittografici, gestione delle vulnerabilità, gestione degli incidenti, controllo della conformità tecnica, test di sicurezza, auditing, raccolta manutenzione e protezione delle prove compresi i registri e le liste di controllo, protezione delle informazioni al termine del contratto di servizio, autenticazione e controllo degli accessi, identità e gestione degli accessi.

1.29. Economics Living Lab 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. Gli incidenti di sicurezza delle informazioni devono essere segnalati al più presto possibile inviando un'e-mail al punto di contatto. Tutte le segnalazioni pervenute saranno gestite per la loro pronta classificazione, rispondendo coerentemente a quanto previsto dalla procedura interna. Il Cliente dovrà sensibilizzare i propri dipendenti affinché forniscano le informazioni appropriate per la gestione dell'incidente da parte di Economics Living Lab. Nel caso in cui l'incidente coinvolga una o più caratteristiche di Riservatezza, Integrità, Disponibilità e Autenticità relativamente ai dati personali; sarà compito del Cliente darne immediata comunicazione ad Economics Living Lab. Ove necessario, ed entro un tempo massimo di 48 ore, deve essere deciso di comune accordo quale delle due parti debba comunicare il *data breach* ed inviare la comunicazione al Garante della Privacy, entro le 72 ore richieste, come previsto dal regolamento UE 2016/679 – GDPR.

1.30. Il Cliente deve richiedere informazioni ad Economics Living Lab riguardo ai meccanismi per: segnalare un eventuale evento di sicurezza che ha rilevato, ricevere segnalazioni riguardanti un evento di sicurezza rilevato da Economics Living Lab, tenere traccia dello stato di un evento di sicurezza segnalato.

1.31. Economics Living Lab esegue regolarmente audit tecnici che consentano di verificare la conformità alle norme ISO/IEC 27001 e relative linee guida ISO 27017 e ISO 27018, nonché consentano il miglioramento continuo del sistema adottato.

1.32. Il Cliente deve considerare che legge e regolamenti pertinenti possono essere quelli delle giurisdizioni che regolano Economics Living Lab, oltre a quelli che regolano lui stesso. Il Cliente dovrà richiedere evidenza della conformità di Economics Living Lab con le normative e gli standard pertinenti richiesti per le proprie attività. Tali prove possono essere le certificazioni prodotti da organismi di terza parte in ambito ISO. A tal proposito Economics Living Lab mette a disposizione eventuali evidenze di certificazione ottenute sul proprio sito istituzionale <https://www.econlivlab.eu/>

1.33. Economics Living Lab effettua il monitoraggio dei servizi cloud con gli strumenti messi a disposizione dal provider; le modifiche a prodotti, servizi e informazioni personali sono storicizzate e conservate attraverso i log di sistema. La protezione dei record raccolti e archiviati viene effettuata con politiche di Economics Living Lab.

1.34. Il Cliente deve definire o estendere le sue politiche procedure esistenti in conformità con il l'uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso dei servizi stessi.

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

1.35. Nella configurazione dei sistemi, Economics Living Lab adotta una propria politica interna basata su logiche di hardening e adottando misure tecniche appropriate. Il Cliente dovrà verificare e garantire che tali aspetti siano appropriati per i propri servizi.

1.36. Alla chiusura di un contratto con Economics Living Lab i servizi del Cliente non saranno più erogati ma i dati non saranno effettivamente cancellati. Dopo 30 giorni dalla disconnessione del servizio, gli asset del Cliente presenti sui sistemi di Economics Living Lab verranno cancellati definitivamente e non potranno più essere recuperati. La riconsegna dei dati al Cliente avverrà in modo sicuro attraverso canali protetti. Avvenuta la restituzione i dati in linea saranno immediatamente eliminati attraverso metodi di cancellazione sicura. I dati di backup rimarranno attivi al più e non oltre 12 mesi per ragioni tecnico organizzative di Economics Living Lab. Il Cliente può comunque richiedere l'eliminazione immediata anche dai dati di backup inviando formale, motivata e giustificata richiesta all'indirizzo del punto di contatto.

1.37. Nel caso in cui siano disponibili funzioni di modifica ai servizi offerti da Economics Living Lab, il Cliente deve documentare e condividere con Economics Living Lab le operazioni previste in caso in cui un errore possa causare danni irreversibili alle risorse nell'ambiente di cloud computing.

ATTENZIONE: Il presente documento è disponibile in copia originale nella sede aziendale. Ogni copia cartacea si ritiene copia di lavoro **non controllata**. È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.