Disposizioni per l'utilizzo di servizi esterni per ospitare o trattare dati e documenti dell'INFN

CCR_SEC_03
Rev. 01 - 24/08/2025

Questo documento indica i criteri in base ai quali gli utenti di risorse informatiche dell'INFN possono utilizzare per la loro attività servizi esterni, inclusi servizi cloud e piattaforme di Intelligenza Artificiale, in funzione della tipologia di dati trattati, per garantire la necessaria riservatezza anche ai fini del trattamento dei dati personali conforme alla disciplina del GDPR.

1. Indicazioni generali

Ove possibile, è sempre preferibile trattare dati utilizzando uno dei servizi interni dell'INFN quali: Alfresco (docs.infn.it), Pandora (pandora.infn.it), INFN GitLab (baltig.infn.it), INFN wiki (confluence.infn.it, wiki.infn.it), etc., o l'utilizzo di applicativi, anche sviluppati esternamente, ma installati su risorse INFN.

Nella scelta di affidarsi ad un servizio esterno è sempre a carico degli utenti considerare con la dovuta attenzione i seguenti aspetti:

- è indispensabile garantire l'accesso ai propri dati per tutto il tempo necessario, anche a lungo termine;
- è necessario valutare le condizioni contrattuali in relazione alla proprietà intellettuale ed ai relativi diritti nell'utilizzo dei dati e delle informazioni esposte;
- è necessario evitare un lock-in, e quindi pianificare una procedura per il recupero dei dati dalla piattaforma esterna in caso di dismissione del servizio

Qualsiasi servizio erogato da fornitore esterno ed utilizzato per attività gestionali o amministrative deve essere certificato dalla Agenzia per la Cybersicurezza Nazionale. Il catalogo dei servizi certificati è consultabile sul sito di ACN[1].

Prima di effettuare qualsiasi acquisto di servizi esterni è necessario consultare il Team responsabile delle risorse informatiche di riferimento, il rappresentante locale in Commissione Calcolo e Reti o l'Ufficio Transizione Digitale, per accertarsi della compatibilità del servizio proposto e verificare che l'esigenza non sia già fruibile attraverso soluzioni sviluppate internamente o su servizi esterni già acquistati centralmente dall'INFN.

2. Dati ordinari

[1] https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

Si intendono dati sostanzialmente pubblici, quali i dati di esperimento o collaborazione, che non abbiano particolari requisiti di riservatezza ed in cui il contenuto di dati personali ordinari sia trascurabile.

Fatto salvo quanto indicato nel paragrafo "**Indicazioni generali**", per questo tipo di dato non ci sono particolari prescrizioni. È utilizzabile qualsiasi risorsa esterna, di collaborazione o commerciale, anche ad uso gratuito.

Esempi:

- strumenti gestiti da organizzazioni con cui l'INFN ha accordi di collaborazione: CERN, EGI, ...
- strumenti e servizi cloud commerciali, anche quando utilizzati in forma gratuita, quali ad esempio i servizi offerti da Amazon, Google, Microsoft, DropBox, GitLab, etc.

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con sistemi esterni di intelligenza artificiale, quali ad esempio OpenAI ChatGPT o Microsoft Copilot, anche in forma gratuita.

3. Dati scientifici riservati

Si intendono dati di tipo tecnico-scientifico che rivestono carattere di riservatezza. Esempi sono:

- dati di esperimento non ancora resi aperti, ad es. dati sotto embargo o con licenza chiusa
- draft di pubblicazioni scientifiche di particolare rilevanza
- progetti tecnologici in attesa di brevetto
- dati coperti da accordi di NDA
- codice sorgente, anche parziale, coperto da una qualsiasi forma di licenza di riutilizzo o comunque di proprietà dell'INFN

Questi dati possono essere trattati su servizi esterni, sia commerciali che non commerciali, per i quali esista un contratto di servizio o un accordo di collaborazione che garantisca il rispetto della riservatezza.

Attualmente i servizi esterni autorizzati sono:

- Piattaforma Office365 su tenant INFN (Microsoft SharePoint, Teams, OneDrive, etc.)
- In caso di dati di proprietà di una collaborazione scientifica, sono autorizzati eventuali sistemi di storage esterni autorizzati dalla collaborazione stessa;

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con i seguenti sistemi di intelligenza artificiale:

- Microsoft Copilot in versione licenziata su tenant INFN

Non è consentita l'elaborazione su sistemi esterni di intelligenza artificiale diversi da quelli indicati, inclusa la versione Copilot su tenant INFN priva di licenza.

È responsabilità dell'utente adottare le misure necessarie a garantire la protezione dei dati adottando configurazioni di permessi o condivisione di link di accesso appropriati.

È necessario considerare le caratteristiche dei servizi utilizzati e mantenere il controllo dei dati in termini di protezione e disponibilità.
In caso di dati condivisi da uffici o collaborazioni è altamente sconsigliato l'utilizzo di aree private, anche in cloud (ad esempio OneDrive); si suggerisce piuttosto di usare aree condivise (ad esempio SharePoint) per evitare la perdita di dati al momento della chiusura di un account.

È altresì necessario che le aree in cloud esterne siano utilizzate solo per la fase di elaborazione di dati e documenti e non per l'eventuale conservazione a lungo termine, per la quale è disponibile il sistema documentale dell'ente, fornito di sistema di backup.

4. Dati personali e dati particolari non genetici

Si intendono i dati in cui sia rilevante la componente di dati personali ordinari, o che contengono dati personali particolari non genetici.

Esempi sono:

- documenti di commissioni di concorso
- documenti connessi a procedure di procurement
- documenti gestiti dalle Direzioni di AC
- documenti gestiti dai servizi del personale
- documenti gestiti dai servizi di prevenzione e protezione
- dati relativi ad accounting e monitoring sull'utilizzo dei sistemi informatici dell'INFN da parte degli utenti di tali sistemi
- dati trattati per garantire la sicurezza dei sistemi informatici dell'INFN, quali quelli relativi all'end point protection, alla threat analysis, etc.

La gestione di questi dati richiede il rispetto delle norme relative al GDPR, che possono essere garantite solo da servizi interni o da servizi esterni contrattualizzati e che siano certificati come idonei ad ospitare servizi cloud per la Pubblica Amministrazione o per i quali sia stata fatta una valutazione del rischio che verifichi i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati e i profili di responsabilità nel trattamento e definito la qualificazione dei rapporti in relazione alla disciplina del GDPR.

Per garantire il più elevato grado di sicurezza, questi dati devono essere conservati su sistemi interni all'Ente o tramite l'utilizzo di applicativi, anche sviluppati esternamente, ma installati su risorse INFN.

È consentito l'utilizzo di servizi esterni, comunque qualificati come sopra descritto, solo per motivi di necessità, quali l'esternalizzazione di un servizio (es: stipendiale, end point protection), o la condivisione in fase di elaborazione dei dati con strumenti o in ambiti non coperti dai sistemi interni.
È responsabilità dell'utente adottare le misure necessarie a garantire la protezione

dei dati adottando configurazioni di permessi o condivisione di link di accesso appropriati.

Si richiede comunque che i dati vengano rimossi dalla piattaforma esterna al termine della fase di elaborazione, e depositati per l'archiviazione a lungo termine su sistemi interni quali ad esempio Alfresco (https://docs.infn.it).

I servizi cloud esterni attualmente autorizzati sono:

- Zucchetti (limitatamente allo stipendiale)
- Piattaforma Office365 su tenant INFN (SharePoint, Teams, ...)
- Microsoft End Point Protection (solo su tenant INFN)

L'utilizzo di Microsoft OneDrive o altre aree personali per dati e documenti condivisi da uffici o collaborazioni è fortemente sconsigliato per gli stessi motivi indicati precedentemente.

È autorizzata l'elaborazione di documenti contenenti tale tipologia di dati con i seguenti sistemi di intelligenza artificiale:

- Microsoft Copilot in versione licenziata, su tenant INFN

Non è consentita l'elaborazione su sistemi esterni di intelligenza artificiale diversi da quelli indicati, inclusa la versione Copilot su tenant INFN priva di licenza.

5. Dati genetici

Nel caso di trattamento di dati genetici deve essere garantita, oltre alle disposizioni previste dal GDPR, la normativa nazionale di attuazione.

A tale scopo, il trattamento su servizi esterni di dati genetici, anche a fini di ricerca, può essere autorizzato solo su infrastrutture o servizi cloud **esplicitamente qualificati allo scopo**, tramite certificazioni o dichiarazioni di idoneità emesse dalle istituzioni nazionali preposte (ACN).

Non è consentito il trattamento di dati genetici su piattaforme esterne di intelligenza artificiale, anche se coperte da contratto INFN.