Provisions for the Use of External Services to Host or Process INFN Data and Documents

CCR_SEC_03
Rev. 01 - 24/08/2025

This document sets out the criteria under which users of INFN IT resources may use external services for their activities, including cloud services and Artificial Intelligence platforms, depending on the type of data processed, to ensure an adequate level of confidentiality, including for the processing of personal data in compliance with the GDPR.

1. General guidelines

Whenever possible, it is always preferable to process data using one of INFN's internal services, such as Alfresco (docs.infn.it), Pandora (pandora.infn.it), INFN GitLab (baltig.infn.it), INFN Wiki (confluence.infn.it, wiki.infn.it), or by using applications, even if externally developed, that are installed on INFN resources.

When relying on an external service, users are required to carefully consider the following aspects:

- it is essential to ensure continued access to data for as long as necessary, including in the long term;
- contractual terms relating to intellectual property and the associated rights concerning the use of data and information made available must be carefully evaluated;
- vendor lock-in must be avoided; therefore, a procedure for retrieving data from the external platform in the event of service discontinuation must be planned.

Any service provided by an external supplier and used for administrative or management activities must be certified by the Italian National Cybersecurity Agency (ACN). The catalogue of certified services is available on the ACN website.

Before purchasing any external service, users must consult the relevant IT resources responsible team, the local representative on the Computing and Networks Commission, or the Digital Transition Office, in order to verify service compatibility and to ensure that the required functionality is not already available through internally developed solutions or external services centrally procured by INFN.

2. Ordinary data

Ordinary data refers to data that is essentially public, such as experimental or collaboration data, which does not have specific confidentiality requirements and for which the presence of ordinary personal data is negligible.

Without prejudice to the provisions set out in the section "**General Guidelines**", no specific restrictions apply to this type of data. Any external resource, whether collaborative or commercial, including free services, may be used.

Examples:

- tools managed by organizations with which INFN has collaboration agreements (e.g. CERN, EGI, ...);
- commercial cloud tools and services, including those offered free of charge, such as services provided by Amazon, Google, Microsoft, Dropbox, GitLab, etc.

Processing documents containing this type of data using external artificial intelligence systems, such as OpenAI ChatGPT or Microsoft Copilot, including free versions, is permitted.

3. Confidential scientific data

Confidential scientific data refers to technical and scientific data that is subject to confidentiality requirements. Examples include:

- experimental data not yet publicly released (e.g. data under embargo or subject to closed licenses);
- drafts of scientific publications of particular relevance;
- technological pending patent applications;
- data covered by non-disclosure agreements (NDAs);
- source code, including partial code, subject to any form of reuse license or owned by INFN.

Such data may be processed on external services, whether commercial or non-commercial, provided that a service contract or collaboration agreement is in place that ensures confidentiality.

The currently authorized external services are:

- Office 365 platform on the INFN tenant (Microsoft SharePoint, Teams, OneDrive, etc.);
- in the case of data owned by a scientific collaboration, external storage systems authorized by the collaboration itself.

Processing documents containing this type of data using the following artificial intelligence systems is authorized:

- Microsoft Copilot, licensed version, on the INFN tenant.

Processing on external artificial intelligence systems other than those listed above is not permitted, including unlicensed versions of Copilot on the INFN tenant.

Users are responsible for adopting appropriate measures to ensure data protection, including the correct configuration of permissions and access-sharing links.

It is necessary to consider the characteristics of the services used and to retain control over data protection and availability.

When data is shared by offices or collaborations, the use of private areas—even in cloud environments (e.g. OneDrive)—is strongly discouraged. Shared areas (e.g. SharePoint) should be used instead, to avoid data loss when an account is closed.

External cloud areas must be used exclusively for data and document processing phases and not for long-term storage, for which INFN's document management system—equipped with a backup system—is available.

4. Dati Personal Data and Special Categories of Non-Genetic Data

This category includes data for which the presence of ordinary personal data is significant, or which contains special categories of personal data other than genetic data.

Examples include:

- documents related to recruitment or selection committees;
- documents related to procurement procedures;
- documents managed by AC Directorates;
- documents managed by human resources services;
- documents managed by occupational health and safety services;
- data related to accounting and monitoring of INFN IT resource usage by users;
- data processed to ensure the security of INFN information systems, such as endpoint protection and threat analysis data.

The processing of such data requires compliance with GDPR provisions, which can only be ensured through internal services or through contracted external services that are certified as suitable for hosting cloud services for the Public Administration, or for which a risk assessment has been carried out. Such assessment must verify limitations on data circulation and transfer, the reliability of the provider, the existence of appropriate safeguards for data retention, persistence, and confidentiality, and the allocation of responsibilities under the GDPR.

To ensure the highest level of security, such data must be stored on systems internal to the Institute or by using applications—even if externally developed—that are installed on INFN resources.

The use of external services, duly qualified as described above, is permitted only where necessary, such as for service outsourcing (e.g. payroll, endpoint protection) or for data sharing during processing phases using tools or environments not covered by internal systems.

Users are responsible for adopting appropriate measures to ensure data protection, including correct permission settings and access-sharing configurations.

In all cases, data must be removed from the external platform at the end of the processing phase and deposited for long-term storage on internal systems, such as Alfresco (https://docs.infn.it).

The currently authorized external cloud services are:

- Zucchetti (limited to payroll services);
- Office 365 platform on the INFN tenant (SharePoint, Teams, etc.);
- Microsoft Endpoint Protection (INFN tenant only).

The use of Microsoft OneDrive or other personal areas for data and documents shared by offices or collaborations is strongly discouraged, for the same reasons outlined above.

Processing documents containing this type of data using the following artificial intelligence systems is authorized:

- Microsoft Copilot, licensed version, on the INFN tenant.

Processing on external artificial intelligence systems other than those listed above is not permitted, including unlicensed versions of Copilot on the INFN tenant.

5. Genetic data

In the case of processing genetic data, compliance with national implementing legislation must be ensured in addition to the provisions of the GDPR.

For this purpose, the processing of genetic data on external services, including for research purposes, may be authorized only on infrastructures or cloud services **explicitly qualified for this purpose**, through certifications or suitability declarations issued by the competent national authorities (ACN).

Processing genetic data on external artificial intelligence platforms is not permitted, even where such platforms are covered by an INFN contract.