



Polistudium srl
Via Solferino 7, 20121 Milano (Sede legale)
Via Caccini 15, 20124 Milano

info@polistudium.it
polistudium@arubapec.it

C.F. e P.IVA 10279960966 - CUU M5UXCR1
www.polistudium.it

Politica Protezione Dati e Sicurezza Informatica

Rev: v.0 – Data emanazione: 24/9/2025 – Data entrata in vigore 1/1/2026

Scopo

Polistudium si impegna a garantire la protezione dei dati personali e delle informazioni aziendali, assicurando la riservatezza, integrità e disponibilità delle informazioni, in linea con il GDPR e la documentazione predisposta dal Titolare e validata dal Data Protection Officer nominato.

Ambito di applicazione

La politica si applica al Direttore Generale e a tutti i collaboratori, inclusi consulenti continuativi e occasionali, che trattano dati e informazioni aziendali, nonché a tutti i soggetti che trattano, con mezzi propri, dati su incarico e nell'interesse di Polistudium e che, a tale scopo, siano stati nominati Responsabili ex art. 28 Reg. Ue 2016/679 (GDPR) e adeguatamente istruiti

Per quanto qui non contenuto si rinvia alla documentazione Privacy in possesso di Polistudium e in corso di aggiornamento.

Principi

Polistudium si impegna a:

- Proteggere i dati personali trattati, adottando misure tecniche ed organizzative adeguate alla natura dei dati, garantendo maggior tutela ai dati particolari ex art. 9 del Reg. Ue 2016/679
- Garantire accessi controllati e tracciabili alle informazioni
- Prevenire accessi non autorizzati, perdita o uso improprio dei dati
- Utilizzare strumenti digitali affidabili e sicuri, secondo i principi di privacy by design e privacy by default
- Adottare un approccio risk based e proattivo, garantendo l'aggiornamento delle misure adottate al variare dell'organizzazione o del rischio
- Rispettare il principio di accountability

Gestione dei dati

- Raccolta e trattamento dei dati limitati a quanto strettamente necessario per le finalità perseguite (principio di minimizzazione)
- Accesso ai dati secondo il principio del minor privilegio
- Conservazione dei dati per il tempo strettamente necessario
- Protezione dei dati tramite strumenti adeguati (password, autenticazione, backup) e mediante politiche di sicurezza
- Adozione di procedure di business continuity e disaster recovery

**Polistudium srl**

Via Solferino 7, 20121 Milano (Sede legale)
Via Caccini 15, 20124 Milano

info@polistudium.it
polistudium@arubapec.it

C.F. e P.IVA 10279960966 - CUU M5UXCR1
www.polistudium.it

Sicurezza nel lavoro remoto

- Utilizzo di dispositivi e connessioni sicure
- Protezione delle credenziali di accesso
- Attenzione alla gestione dei dati
- Utilizzo preferenziale di piattaforme cloud affidabili

Obiettivi

- Garantire che tutti i collaboratori siano informati sulle buone pratiche di sicurezza informatica
- Monitorare il rispetto delle policy
- Zero incidenti significativi di sicurezza dei dati non gestiti (corretta e tempestiva gestione dei data breach e dei near miss)

Modalità di attuazione

- Condivisione di linee guida sulla sicurezza informatica
- Utilizzo di strumenti con standard adeguati di sicurezza
- Aggiornamento periodico delle pratiche di sicurezza
- Test di vulnerabilità e verifica piano d'azione di business continuity

Segnalazione incidenti

- Eventuali incidenti o rischi relativi ai dati devono essere segnalati tempestivamente alla Direzione Generale o all'amministratore di sistema, che, con il supporto del Data Protection Officer, compie l'istruttoria interna e adotta le contromisure urgenti e quelle di sistema, secondo la procedura in tema di data breach ed incidenti di sicurezza
- È garantita la riservatezza delle segnalazioni

Monitoraggio

Polistudium monitora:

- Eventuali incidenti o vulnerabilità
- Adozione delle buone pratiche di sicurezza

Revisione

La politica è revisionata ogni 3 anni o nel minor tempo fissato dal Registro dei Trattamenti o altro.

Il Direttore Generale
Luca Giacomelli

**Polistudium srl**

Via Solferino 7, 20121 Milano (Sede legale)
Via Caccini 15, 20124 Milano

info@polistudium.it
polistudium@arubapec.it

C.F. e P.IVA 10279960966 - CUU M5UXCR1
www.polistudium.it

Data Protection and Information Security Policy

Rev.: v.0 – Issue Date: 24/09/2025 – Effective Date: 01/01/2026

Purpose

Polistudium is committed to ensuring the protection of personal data and company information, safeguarding the confidentiality, integrity, and availability of information, in compliance with the GDPR and the documentation prepared by the Data Controller and validated by the appointed Data Protection Officer.

Scope

This policy applies to the General Manager and all collaborators, including ongoing and occasional consultants, who process company data and information, as well as to all parties who process data on behalf of and in the interest of Polistudium using their own means and who, for this purpose, have been appointed as Data Processors pursuant to Article 28 of EU Regulation 2016/679 (GDPR) and have received appropriate instructions.

For matters not covered herein, reference is made to the Privacy documentation held by Polistudium and currently being updated.

Principles

Polistudium undertakes to:

- Protect the personal data processed by adopting technical and organizational measures appropriate to the nature of the data, ensuring enhanced protection for special categories of data pursuant to Article 9 of EU Regulation 2016/679.
- Ensure controlled and traceable access to information.
- Prevent unauthorized access, loss, or misuse of data.
- Use reliable and secure digital tools in accordance with the principles of privacy by design and privacy by default.
- Adopt a risk-based and proactive approach, ensuring that the measures adopted are updated in response to organizational or risk changes.
- Comply with the principle of accountability.

Data Management

- Collection and processing of data limited to what is strictly necessary for the intended purposes (principle of data minimization).
- Access to data according to the principle of least privilege.
- Retention of data only for the time strictly necessary.
- Protection of data through appropriate tools (passwords, authentication, backups) and security policies.
- Adoption of business continuity and disaster recovery procedures.

Security in Remote Work

- Use of secure devices and connections.
-

**Polistudium srl**

Via Solferino 7, 20121 Milano (Sede legale)
Via Caccini 15, 20124 Milano

info@polistudium.it
polistudium@arubapec.it

C.F. e P.IVA 10279960966 - CUU M5UXCR1
www.polistudium.it

- Protection of access credentials.
- Careful management of data.
- Preferential use of reliable cloud platforms.

Objectives

- Ensure that all collaborators are informed about good cybersecurity practices.
- Monitor compliance with policies.
- Achieve zero unmanaged significant data security incidents (including proper and timely management of data breaches and near misses).

Implementation Methods

- Sharing of cybersecurity guidelines.
- Use of tools with adequate security standards.
- Periodic updating of security practices.
- Vulnerability testing and verification of the business continuity action plan.

Incident Reporting

- Any incidents or risks related to data must be promptly reported to the General Management or the system administrator who, with the support of the Data Protection Officer, will carry out the internal investigation and adopt urgent and systemic countermeasures in accordance with the procedure concerning data breaches and security incidents.
- Confidentiality of reports is guaranteed.

Monitoring

Polistudium monitors:

- Any incidents or vulnerabilities.
- Adoption of good security practices.

Review

This policy is reviewed every 3 years or within the shorter timeframe established by the Record of Processing Activities or other applicable requirements.

The General Director

Luca Giacomelli