I fornitori di servizi cloud che intendono operare con la Pubblica Amministrazione italiana devono soddisfare requisiti di sicurezza e conformità specifici, definiti principalmente dall'**Agenzia per l'Italia Digitale (AgID)** e dal **Regolamento sul Cloud della PA**. Questi requisiti includono una serie di certificazioni e attestazioni riconosciute a livello nazionale e internazionale.

Ecco un riepilogo delle certificazioni richieste:

---

1. Certificazioni di Sicurezza e Qualità

I fornitori devono dimostrare di essere conformi a standard internazionali che garantiscano sicurezza, qualità, e affidabilità del servizio. Le certificazioni più comuni sono:

ISO/IEC 27001

- Certificazione di riferimento per la gestione della sicurezza delle informazioni.
- È obbligatoria per garantire la protezione dei dati sensibili e il rispetto delle normative in materia di sicurezza.

ISO/IEC 27017

- Standard specifico per la sicurezza nei servizi cloud.
- Include linee guida per la gestione sicura dell'infrastruttura e dei dati nel cloud.

ISO/IEC 27018

- Standard per la protezione dei dati personali nei servizi cloud.
- Garantisce che i fornitori rispettino i principi di privacy e trasparenza.

ISO 22301

- Standard per la gestione della continuità operativa.
- Richiesto per assicurare che il servizio cloud sia resiliente e possa operare anche in situazioni di emergenza.

---

2. Qualificazione AgID

I fornitori di servizi cloud devono ottenere la **qualificazione AgID** per poter offrire servizi alla Pubblica Amministrazione. Questo processo prevede:

- **Requisiti organizzativi e finanziari**: dimostrazione di solidità aziendale.
- **Requisiti di sicurezza**: implementazione di controlli di sicurezza e protezione dati.
- **Requisiti di interoperabilità e portabilità**: capacità di garantire che i dati siano facilmente trasferibili e accessibili.

---

3. Conformità al Regolamento Europeo

GDPR (General Data Protection Regulation)

- Tutti i fornitori devono rispettare il **Regolamento UE 2016/679**, che disciplina la protezione dei dati personali.
- È essenziale che i fornitori abbiano implementato politiche e misure di sicurezza adeguate per trattare i dati sensibili.

---

4. Certificazioni di Cloud Security Specifiche

CISPE Code of Conduct

- Codice di condotta per i fornitori di infrastrutture cloud, conforme al GDPR.
- Dimostra l'impegno per la protezione dei dati e la trasparenza.

CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry)

- Certificazione che garantisce un alto livello di sicurezza e trasparenza nei servizi cloud.

---

5. Requisiti di Sovranità dei Dati

- I fornitori devono garantire che i dati siano ospitati in infrastrutture conformi alle normative italiane ed europee.
- In alcuni casi, è richiesto che i dati siano gestiti in **data center situati in Italia** o in altri Paesi UE.

---

6. Altri Requisiti Specifici

- **Accesso selettivo ai dati**: garanzia che solo personale autorizzato possa accedere ai dati della Pubblica Amministrazione.
- **Audit e monitoraggio continuo**: possibilità di verificare periodicamente i controlli di sicurezza implementati.
- **Compliance con il Piano Triennale per l'Informatica nella Pubblica Amministrazione**.

Risorse Utili

- **Catalogo dei Servizi Cloud per la PA**: Fornitori qualificati e servizi approvati sono pubblicati nel catalogo ufficiale AgID (link ufficiale).
- **Documentazione AgID**: Linee guida tecniche e requisiti sono disponibili sul sito dell'Agenzia.
