

Codice Aziendale per la Protezione dei Dati Sensibili

Cybersecurity & Data Protection

Sommario

1. Scopo e Ambito di Applicazione	1
2. Riferimenti Normativi e Standard.....	1
3. Tipologie di Informazioni Protette.....	1
4. Principi di Gestione delle Informazioni	2
5. Ruoli e Responsabilità	2
6. Sicurezza Informatica e Protezione dei Sistemi	2
7. Gestione dei Dati di Progetto	2
8. Dispositivi Aziendali e Lavoro da Remoto	2
9. Cantieri, Sopralluoghi e Attività sul Campo.....	2
10. Gestione degli Incidenti e Data Breach.....	3
11. Fornitori, Consulenti e Partner.....	3
12. Formazione e Cultura della Sicurezza.....	3
13. Violazioni e Provvedimenti	3
14. Revisione e Aggiornamento.....	3

1. Scopo e Ambito di Applicazione

Il presente Codice stabilisce i principi e le misure adottate dalla TPS Ingegneria srl per garantire la sicurezza delle informazioni, la protezione dei dati personali e la riservatezza delle informazioni tecniche e progettuali trattate nello svolgimento delle proprie attività.

Il Codice si applica a:

- Soci, amministratori e dirigenti
- Dipendenti, collaboratori, consulenti, tirocinanti
- Partner tecnici, subappaltatori e fornitori
- Tutti i dati e le informazioni trattate nell'ambito dei servizi di ingegneria, in formato digitale e cartaceo
- Tutti i sistemi informativi, le piattaforme di progetto e gli archivi aziendali

2. Riferimenti Normativi e Standard

La società opera in conformità a:

- Regolamento (UE) 2016/679 (GDPR)
- Normativa nazionale sulla protezione dei dati
- Norme su segreto professionale e proprietà intellettuale
- Best practice di sicurezza delle informazioni (ISO/IEC 27001, ISO 19650 – BIM)

3. Tipologie di Informazioni Protette

La Società tratta, in particolare:

- **Dati personali** (clienti, dipendenti, fornitori)
- **Dati particolari** (sicurezza cantieri, idoneità sanitarie)
- **Dati tecnici e progettuali riservati** (elaborati grafici, modelli BIM, calcoli, relazioni, computi)
- **Dati infrastrutturali critici**
- **Informazioni economiche, contrattuali e strategiche**

Tali dati sono considerati **informazioni sensibili e strategiche** e devono essere adeguatamente protetti.

Tutte le informazioni di progetto sono considerate **confidenziali**, salvo diversa indicazione contrattuale.

4. Principi di Gestione delle Informazioni

La Società opera secondo i seguenti principi:

- Riservatezza e segreto professionale
- Protezione della proprietà intellettuale
- Accesso ai dati secondo il principio del *need to know*
- Tracciabilità delle attività sui dati di progetto
- Continuità operativa dei sistemi informativi

5. Ruoli e Responsabilità

- **Titolare del Trattamento:** TPS Ingegneria srl nella persona del suo Amm.Unico Ing. Ernesto Martegiani
- **Responsabile IT e Cybersecurity:** garantisce sicurezza e continuità dei sistemi
- **DPO / Referente Privacy (se nominato):** supervisiona la conformità GDPR
- **Project Manager / Responsabile di Commessa:** assicura la corretta gestione e condivisione dei dati di progetto
- **Utenti Autorizzati:** utilizzano i dati solo per finalità lavorative

Ogni soggetto è responsabile della protezione delle informazioni a cui ha accesso.

6. Sicurezza Informatica e Protezione dei Sistemi

La Società adotta misure tecniche e organizzative quali:

- Autenticazione forte (MFA) per sistemi e accessi remoti
- Gestione centralizzata degli account e dei permessi
- Protezione dei server di progetto e ambienti BIM
- Crittografia dei dati sensibili e dei backup
- Aggiornamento e patching continuo dei software tecnici
- Sistemi di backup, versioning e disaster recovery

7. Gestione dei Dati di Progetto

- I dati di progetto sono archiviati esclusivamente su sistemi aziendali autorizzati
- È vietato l'uso di dispositivi e cloud personali non autorizzati
- La condivisione con clienti e partner avviene solo tramite piattaforme sicure
- Ogni modifica agli elaborati deve essere tracciabile e versionata
- Al termine della commessa i dati vengono archiviati o distrutti secondo policy

8. Dispositivi Aziendali e Lavoro da Remoto

- I dispositivi aziendali devono essere protetti da password, cifratura e antivirus
- Il lavoro da remoto è consentito solo tramite VPN e strumenti autorizzati
- È vietata la memorizzazione locale non protetta di dati di progetto
- In caso di smarrimento o furto, il dispositivo deve essere segnalato immediatamente

9. Cantieri, Sopralluoghi e Attività sul Campo

- Foto, rilievi e documentazione tecnica sono dati riservati
- I dati raccolti in campo devono essere trasferiti su sistemi aziendali protetti
- I documenti cartacei devono essere custoditi e smaltiti in modo sicuro
- È vietata la diffusione non autorizzata di informazioni tecniche

10. Gestione degli Incidenti e Data Breach

In caso di incidente informatico o violazione dei dati:

1. Segnalazione immediata al Responsabile IT/Privacy
2. Attivazione delle procedure di contenimento
3. Analisi dell'impatto su dati personali e di progetto
4. Notifica alle Autorità e agli interessati, se previsto dalla normativa

11. Fornitori, Consulenti e Partner

- Devono rispettare le stesse misure di sicurezza della Società
- Sono vincolati da NDA e accordi sul trattamento dei dati
- Possono accedere solo ai dati strettamente necessari
- Sono soggetti a verifiche di conformità

12. Formazione e Cultura della Sicurezza

La Società promuove:

- Formazione obbligatoria su cybersecurity e privacy
- Aggiornamenti periodici sui rischi informatici
- Sensibilizzazione sulla protezione dei dati di progetto

13. Violazioni e Provvedimenti

La violazione del presente Codice può comportare:

- Sanzioni disciplinari
- Responsabilità contrattuali e professionali
- Azioni legali e segnalazioni alle Autorità competenti

14. Revisione e Aggiornamento

Il Codice è riesaminato periodicamente per garantire:

- Conformità normativa
- Adeguatezza rispetto ai servizi di ingegneria svolti
- Protezione contro nuove minacce informatiche

Teramo, 01/09/2025

TPS INGEGNERIA SRL

Ing. Ernesto Martegiani


TPS INGEGNERIA s.r.l.
Via Campana, 4 - 64100 TERAMO
Tel. 0861.246130 - P. I. 00961200672