COLLEGIO DEI GEOMETRI E GEOMETRI LAUREATI DELLA PROVINCIA DI PISA

Regolamento interno per l'utilizzo delle postazioni informatiche della segreteria e la gestione degli accessi ai dati personali

PREMESSA

Il presente Regolamento disciplina l'utilizzo delle postazioni informatiche, degli account di posta elettronica, delle reti e dei sistemi informatici del Collegio dei Geometri e Geometri Laureati della Provincia di Pisa, garantendo la conformità alle disposizioni del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e s.m.i. (Codice Privacy) e ai provvedimenti del Garante per la Protezione dei Dati Personali.

ART. 1 – TITOLARE DEL TRATTAMENTO, DPO E RUOLI PRIVACY

1. **Titolare del Trattamento:** Il Titolare del trattamento dei dati personali è il **Collegio dei Geometri e Geometri Laureati della Provincia di Pisa**, in persona del Presidente pro tempore.
2. **Data Protection Officer (DPO / RPD):** Il Responsabile della Protezione dei Dati designato dal Collegio è il **Dott. Niccolò Paperini** (Autem S.r.l.).
3. **Referente Privacy Interno:** Il **Geom. Stefano Fattorini** opera in qualità di *Referente Privacy Interno* del Collegio, con compiti di raccordo organizzativo interno, vigilanza operativa e supporto all'attuazione delle direttive impartite dal Titolare e dal DPO.
4. **Soggetti Autorizzati al trattamento:** I dipendenti, i consiglieri e i collaboratori interni operano quali *Soggetti autorizzati al trattamento* ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003 e s.m.i., previa ricezione

di formale lettera di designazione individuale contenente le istruzioni specifiche relative alle mansioni assegnate.

ART. 2 – SOGGETTI AUTORIZZATI E STRUTTURA ORGANIZZATIVA

Sono definiti soggetti autorizzati all'utilizzo delle risorse informatiche e al trattamento dei dati personali, nei limiti delle rispettive competenze istituzionali:

- **Presidente:** Andrea Pieracci
- **Segretario:** Cristian Parente
- **Tesoriere:** Francesco Bertelli
- **Consigliere:** Francesco Salani
- **Consigliere:** Alessandro Malvaldi
- **Referente Privacy Interno:** Stefano Fattorini
- **Segretaria Amministrativa:** Annalisa Antoni

ART. 3 – PROFESSIONISTI ED OPERATORI ESTERNI (RESPONSABILI EX ART. 28 GDPR)

1. Il Dott. **Luca Zucchelli** (Contabile esterno) opera in qualità di **Responsabile Esterno del Trattamento** ai sensi dell'art. 28 del GDPR.
2. Il rapporto di trattamento dati con il Dott. Luca Zucchelli è disciplinato da un apposito atto contrattuale/nomina scritta ex art. 28 GDPR, che definisce dettagliatamente l'oggetto, la durata, la natura del trattamento, le istruzioni documentate del Titolare, gli obblighi di riservatezza, le misure di sicurezza tecniche e organizzative adottate, la gestione dei data breach e l'eventuale ricorso a sub-responsabili.

ART. 4 – ASSEGNAZIONE DELLE POSTAZIONI INFORMATICHE E SEGREGAZIONE DEGLI ACCOUNT

1. Postazioni di Segreteria (N° 2 PC - Uso esclusivo):
    - *Utilizzatori autorizzati:* Annalisa Antoni e Cristian Parente.
    - *Ambito di trattamento:* Posta elettronica istituzionale, protocollo, pratiche amministrative, anagrafica iscritti e documentazione riservata del Collegio.
2. Postazione Condivisa "Contabilità e Gestione Crediti Formativi":
    - Al fine di garantire il principio di responsabilizzazione (*accountability*, art. 5.2 GDPR) e la segregazione degli accessi, sulla postazione condivisa sono configurati **profili utente/account personali e distinti** a livello di sistema operativo:
        - **Account "Luca Zucchelli" (Professionista Esterno):** Accesso limitato ed esclusivo alla cartella/software per i soli dati amministrativi e contabili.
        - **Account "Alessandro Malvaldi" (Consigliere):** Accesso riservato alla gestione e caricamento dei crediti formativi per i corsi di prevenzione incendi.
        - **Account "Francesco Salani" (Consigliere):** Accesso riservato alla gestione e caricamento dei crediti formativi per gli altri corsi di formazione.
    - È fatto espresso divieto di utilizzare account generici o condivisi.
3. Dispositivi del Presidente e del Tesoriere / Policy BYOD:
    - Il Presidente (Andrea Pieracci), il Segretario (Cristian Parente) e il Tesoriere (Francesco Bertelli) operano tramite postazioni istituzionali o, ove utilizzino dispositivi personali per finalità istituzionali (Bring Your Own Device - BYOD):

- Devono garantire l'adozione di misure minime di sicurezza sul dispositivo (sistema operativo aggiornato, antivirus attivo, blocco schermo protetto da credenziali/PIN/biometria e cifratura del disco).
- Le credenziali dell'account istituzionale non devono essere salvate in chiaro o condivise con terzi/familiari.

ART. 5 – GESTIONE DELLA POSTA ELETTRONICA ISTITUZIONALE

1. L'accesso e l'utilizzo della casella di posta elettronica istituzionale del Collegio sono consentiti esclusivamente agli utenti autorizzati **Annalisa Antoni** e **Cristian Parente**.
2. **Verifica e Bonifica Tecnica:** Il Collegio garantisce, tramite verifiche tecniche periodiche, che l'account di posta istituzionale sia configurato esclusivamente sulle postazioni della Segreteria. È rimossa ogni configurazione, credenziale memorizzata o reindirizzamento automatizzato su PC o dispositivi non espressamente autorizzati.
3. È vietato comunicare le credenziali della posta a soggetti non autorizzati o utilizzare l'account per finalità extra-istituzionali.

ART. 6 – AMMINISTRATORE DI SISTEMA E GESTIONE DEI PRIVILEGI

1. **Designazione:** In adempimento al Provvedimento del Garante del 27 novembre 2008, il Collegio individua e formalizza la nomina degli Amministratori di Sistema (interni o fornitori IT esterni), tenendo un elenco aggiornato ed esposto/consultabile.
2. **Log degli Accessi:** Vengono attivati e conservati i log di accesso degli Amministratori di Sistema per un periodo non inferiore a 6 (sei) mesi, garantendone l'infallibilità e l'integrità.

3. **Privilegi Utente Standard:** Tutti i soggetti autorizzati operano sulle rispettive postazioni di lavoro con un **account a privilegi standard (non amministratore)**.
4. I privilegi di Amministratore Locale sono riservati esclusivamente all'Amministratore di Sistema. Eventuali esigenze di installazione di software o modifiche di configurazione devono essere formalmente richieste all'Amministratore di Sistema.

ART. 7 – SICUREZZA INFORMATICA E CUSTODIA DELLE CREDENZIALI

Tutti i soggetti autorizzati devono attenersi alle seguenti misure di sicurezza:

1. **Credenziali di Accesso:**
    - Le password devono contenere almeno 12 caratteri, comprendenti lettere maiuscole, minuscole, numeri e caratteri speciali.
    - La modifica della password è obbligatoria ogni 90 giorni (o al primo accesso).
    - Ove disponibile, è obbligatoria l'attivazione dell'Autenticazione a Più Fattori (MFA).
    - Le credenziali sono strettamente personali e confidate sotto la responsabilità dell'utente.
2. **Blocco Postazione:**
    - La postazione deve essere bloccata manualmente (es. Win + L) ogni volta che l'utente si allontana dal posto di lavoro.
    - È impostato il blocco automatico dello schermo per inattività decorso un intervallo massimo di 10 minuti.
3. **Aggiornamenti e Antivirus:**
    - I sistemi operativi, gli antivirus e i software applicativi sono soggetti ad aggiornamenti automatici e periodici curati dall'Amministratore di Sistema.

4. **Backup e Continuità Operativa:**
    - I backup dei dati del Collegio vengono effettuati con cadenza giornaliera/settimanale secondo la procedura definita dall'Amministratore di Sistema, con verifica periodica della ripristinabilità dei dati (*disaster recovery*).
5. **VPN e Accessi da Remoto:**
    - L'accesso da remoto ai sistemi del Collegio è consentito unicamente tramite connessioni cifrate sicure (VPN) previa formale autorizzazione.

ART. 8 – REGOLAMENTAZIONE DELL'USO DELLE POSTAZIONI E DIVIETI

1. Le postazioni e gli strumenti informatici sono destinati esclusivamente alle attività istituzionali del Collegio.
2. È fatto espresso divieto di:
    - Installare software, estensioni o programmi non espressamente autorizzati.
    - Utilizzare dispositivi di memorizzazione di massa rimovibili (chiavette USB, hard disk esterni) privi di previa autorizzazione e scansione antivirus.
    - Modificare la configurazione hardware, software o di rete delle macchine.
    - Utilizzare i sistemi per scopi personali, illeciti o incompatibili con il decoro e la sicurezza dell'Ente.
3. Sanzioni Disciplinari: La violazione delle prescrizioni del presente Regolamento costituisce illecito disciplinare e/o contrattuale e comporterà l'applicazione delle sanzioni previste dai contratti di lavoro o dalle norme ordinistiche (richiamo, sospensione o revoca dei profili di accesso, fino alle conseguenze di legge).

ART. 9 – PROCEDURA OPERATIVA IN CASO DI DATA BREACH

1. **Segnalazione Interna Immediata:** Chiunque rilevi o sospetti un incidente di sicurezza (es. furto/smarrimento di PC o chiavette USB, attacco ransomware, invio errato di email con dati sensibili a terzi) deve segnalarlo immediatamente al Referente Privacy Interno e al DPO (Dott. Niccolò Paperini).
2. **Procedura e Tempistiche di Notifica:**
    - Il DPO e il Titolare valutano il rischio per i diritti e le libertà delle persone fisiche.
    - Qualora sia probabile un rischio, il Titolare provvede alla **notifica al Garante per la Protezione dei Dati Personali entro 72 ore** dalla conoscenza dell'evento (art. 33 GDPR).
    - Qualora il rischio sia elevato, il Titolare provvede a **comunicare l'evento tempestivamente agli interessati** coinvolti (art. 34 GDPR).
3. **Registro dei Data Breach:** Tutte le violazioni, anche quelle non notificate al Garante, sono documentate in un apposito Registro interno delle violazioni di dati personali.

ART. 10 – CONSERVAZIONE E MINIMIZZAZIONE DEI DATI

1. I dati personali trattati tramite le postazioni informatiche (anagrafica iscritti, protocollo, gestione contabile, crediti formativi, corrispondenza) sono gestiti nel rispetto del principio di minimizzazione ex art. 5.1.c GDPR.
2. I tempi di conservazione dei dati (*data retention*) per ciascuna tipologia di trattamento sono stabiliti e dettagliati all'interno del **Registro delle Attività di Trattamento** del Collegio (art. 30 GDPR), a cui si fa espresso rinvio.

ART. 11 – FORMAZIONE PERIODICA DEL PERSONALE

1. Il Collegio promuove ed organizza **sessioni di formazione obbligatoria e periodica** (con cadenza almeno annuale) per tutti i soggetti autorizzati al trattamento.
2. La formazione ha ad oggetto le norme sul GDPR, i rischi della sicurezza informatica (es. *phishing*, *social engineering*) e le buone prassi operative.
3. La partecipazione alle sessioni formative viene formalmente tracciata e verbalizzata.

ART. 12 – EFFICACIA, REVISIONE E APPROVAZIONE

1. **Parere del DPO:** Il presente Regolamento è adottato previo parere obbligatorio (seppur non vincolante) reso dal Data Protection Officer (DPO).
2. **Approvazione ed Entrata in Vigore:** Il Regolamento entra formalmente in vigore a seguito dell'approvazione con Delibera del Consiglio del Collegio e previa sottoscrizione per presa visione ed accettazione da parte di tutti i soggetti autorizzati.
3. **Revisione Periodica:** Il presente Regolamento è soggetto a **revisione con cadenza almeno annuale**, oppure in presenza di significative modifiche organizzative, normative o tecnologiche.

MODULO DI SOTTOSCRIZIONE PER PRESA VISIONE ED ACCETTAZIONE

I sottoscritti dichiarano di aver ricevuto, letto e compreso il presente Regolamento interno, impegnandosi a rispettarne integralmente il contenuto e le istruzioni ricevute.

Firma per presa visione

Nominativo	Firma	Data
Andrea Pieracci		
Cristian Parente		
Francesco Bertelli		
Francesco Salani		
Alessandro Malvaldi		
Luca Zucchelli		
Stefano Fattorini (Delegato Privacy)		
Annalisa Antoni		