REGOLAMENTO PRIVACY DELL'ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ALESSANDRIA

Regole di comportamento riguardo il trattamento dei dati personali e aziendali, gli strumenti ed i sistemi informatici

Approvato con delibera del Consiglio dell'Ordine in data 05/09/18

INDICE

I. INTRODUZIONE

1.PREMESSA

Il presente Regolamento è emanato con atto del Consiglio dell'Ordine al fine di individuare le norme comportamentali e le procedure tecnico-organizzative cui è necessario attenersi in materia di trattamento di dati personali e di sicurezza nello svolgimento di tutte le attività istituzionali dell'Ordine degli ingegneri della provincia di Alessandria (di seguito anche "Ordine")
In particolare, si ritiene necessario definire una chiara disciplina interna atta garantire che il trattamento dei dati personali svolto nell'ambito delle mansioni lavorative, avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. TUTELA DEL LAVORATORE

Il luogo di lavoro è una formazione sociale rispetto alla quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità di ciascuno in modo da garantire, in una cornice di reciproci diritti e doveri, l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

3. SCOPO, CAMPO DI APPLICAZIONE E DESTINATARI

Lo scopo del presente Regolamento è quello di definire un insieme di norme comportamentali a cui tutti i dipendenti, i collaboratori, le eventuali terze parti e - in generale - gli utenti interni ed esterni dell'Ordine degli ingegneri della provincia di Alessandria devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.
Il presente Regolamento è realizzato in conformità a quanto previsto dal Regolamento Europeo n. 2016/679 – General Data Protection Regulation (da ora "GDPR") e dai Provvedimenti del Garante.

Il presente Regolamento è destinato ai seguenti utenti (da ora "Utenti"):

Utenti interni:
- componenti del Consiglio
- dipendenti
- collaboratori coordinati e continuativi
- consulenti e collaboratori occasionali

Utenti esterni:

- componenti del Consiglio di Disciplina
- iscritti
- collaboratori a qualsiasi titolo di imprese fornitrici di beni, servizi o lavori che realizzano opere in favore dell'Ordine
- personale di altre entità presenti nella sede dell'Ordine in forza di convenzioni o accordi inter-istituzionali
- visitatori e ospiti di vario genere

II. DEFINIZIONI

1. Sono di seguito riportate le principali definizioni privacy tratte dal GDPR.

Dato personale: qualsiasi informazione che identifica o rende identificabile una persona fisica e che può fornire dettagli sulle sue caratteristiche fisiche, fisiologiche, genetiche o psichiche, sulle sue abitudini, sul suo stile di vita, sulle sue relazioni personali, sul suo stato di salute o sulla sua situazione economica.

Dati identificativi: dati personali che permettono l'identificazione diretta di una persona fisica.

Dati sensibili: dati personali idonei a rivelare lo stato di salute (attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria) e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale di una persona fisica.

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla sua fisiologia o salute.

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati giudiziari: dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Trattamento di dati personali: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile.

Comunicazione di dati personali: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Diffusione di dati personali: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Violazione di dati personali: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Titolare del trattamento: organizzazione nel suo complesso, nella persona del suo Legale Rappresentante che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Contitolare del trattamento: Titolare del trattamento che determina congiuntamente ad altro Titolare le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR.

Responsabile del trattamento (interno o esterno): persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Sub-responsabile del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare;

Incaricato/autorizzato del trattamento: persona fisica autorizzata a compiere operazioni di trattamento dati, sulla base dei regolamenti adottati dal Titolare e delle istruzioni impartite dal Responsabile del trattamento.

Interessato: persona fisica cui si riferiscono i dati personali trattati.

Amministratore di sistema: persona fisica nominata dal Titolare e preposta alla gestione e sicurezza dei sistemi informativi attraverso l'applicazione delle misure necessarie al mantenimento della riservatezza, disponibilità e integrità del dato personale trattato nei sistemi informativi.

Responsabile della protezione dei dati (Data Protection Officer - DPO): persona fisica nominata dal Titolare che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione privacy definite dal Titolare, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

2. Sono di seguito riportate alcune altre definizioni utili alla corretta gestione dei processi di trattamento dei dati personali.

Strumenti informatici: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.

Cloud Pubblica: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

III. MODELLO ORGANIZZATIVO

1. CLASSIFICAZIONE DELLE INFORMAZIONI

L'Ordine degli ingegneri della provincia di Alessandria classifica il proprio patrimonio informativo (costituito da tutti i dati e le informazioni trattati nei diversi ambiti, tra i quali anche i dati personali) secondo i seguenti criteri:

Dati e informazioni pubbliche: sono le informazioni liberamente trattabili da Utenti attraverso i mezzi di comunicazione messi a disposizione dall'Ordine (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte dell'Utente particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per l'Ordine in quanto si tratta di informazioni pubbliche che possono essere diffuse.

Dati e informazioni interne: sono le informazioni che possono essere trattate dagli Utenti esclusivamente all'interno dei processi e del contesto organizzativo dell'Ordine attraverso i canali istituzionali. Queste informazioni richiedono da parte dell'Utente una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una violazione dei vincoli di riservatezza ai quali è legato ogni Utente con un possibile impatto legale (per esempio, violazione della privacy), a meno di essere rielaborate in modo da essere declassate a livello pubblico.

Dati e informazioni riservate: sono le informazioni che possono essere trattate da gruppi di Utenti autorizzati in virtù del ruolo e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo ad Utenti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione dall'Ordine in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della privacy), d'immagine e istituzionale per l'Ordine.

Dati e informazioni strettamente riservate: sono le informazioni che possono essere trattate esclusivamente da determinati Utenti in base al ruolo ed alle responsabilità ricoperte all'interno dell'Ordine. La divulgazione di tali informazioni può produrre gravi danni legali (per esempio, violazione della privacy), di immagine e istituzionale per l'Ordine.

2. MODELLO ORGANIZZATIVO DI RESPONSABILITÀ PRIVACY

Nell'ambito della conformità al GDPR e sulla base del proprio organigramma, l'Ordine ha definito e formalizzato un Modello Organizzativo di responsabilità privacy finalizzato al corretto trattamento dei dati personali. Il modello è allegato al presente Regolamento e ne costituisce parte integrante (Allegato 1).
Al di là del Modello Organizzativo relativo alle responsabilità privacy di cui sopra, tutti coloro che svolgano una operazione che contempla il trattamento di dati personali - d'intesa con il Titolare e per il tramite del Responsabile della Prevenzione della Corruzione, Trasparenza e DPO – sono tenuti ad adottare una policy *ad hoc* configurata sulle specifiche esigenze del caso (c.d. Privacy by Design).

IV. POLICY DI COMPORTAMENTO

1. PRINCIPI GENERALI DEL TRATTAMENTO

Trattare un dato personale rappresenta qualunque operazione o complesso di operazioni realizzate su un dato personale ed effettuate anche senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo alcuni principi generali privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali. È importante chiedersi sempre se questi vincoli siano rispettati e solo ad una risposta sempre positiva possiamo avere la certezza che la privacy di una persona sia rispettata. In particolare quando avviene un trattamento di dati personali devono sempre essere rispettati i seguenti principi generali:

- **Il rispetto della dignità dell'interessato**, cioè della persona fisica di cui si stanno trattando i dati personali.

- **Il rispetto dei principi di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Quanto alla trasparenza, il linguaggio utilizzato deve essere semplice e chiaro.

- **Il rispetto del principio di limitazione della finalità:** gli scopi del trattamento devono essere determinati, espliciti e legittimi, e successivamente trattati in un modo che non sia incompatibile con tali scopi (salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).

- **Il rispetto del principio di minimizzazione dei dati:** i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità ('principio di necessità').

- **Il rispetto del principio di esattezza**: i dati trattati devono essere esatti e, se necessario, aggiornati, pertanto devono essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto alle finalità per le quali sono trattati.

- **Il rispetto del principio di limitazione della conservazione**: i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati (salvo specifici obblighi di legge, trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).

- **Il rispetto del principio di integrità e riservatezza**: i dati devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti dalla perdita, dalla distruzione e dal danno accidentale.

2. TRATTAMENTO DI DATI RACCOLTI PER SCOPI STATISTICI E DI RICERCA SCIENTIFICA

Gli scopi statistici e di ricerca scientifica devono essere chiaramente determinati e resi noti all'interessato nell'informativa. I dati personali trattati per scopi statistici e di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti finalizzati a scopi di altra natura. Essi sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. I dati identificativi, qualora possano essere conservati, sono abbinabili ad altri dati, sempre che l'abbinamento sia temporaneo ed essenziale per i propri trattamenti statistici. Le disposizioni, relative al segreto statistico e alla riservatezza dei dati personali, non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

3. GESTIONE DEI LOCALI E DELLE RISORSE FISICHE

Tutti i locali e tutte le risorse fisiche dell'Ordine degli ingegneri della provincia di Alessandria devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni, attenendosi al presente Regolamento per garantire la sicurezza fisica di aree ed *asset* dell'Ordine.

4. ACCESSO AGLI UFFICI ED AREE PROTETTE

Sede e uffici. L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso agli Utenti autorizzati, in base a precise e motivate esigenze lavorative.

Segreteria. L'accesso è consentito a visitatori e ospiti di vario genere, che possono posizionarsi appoggiandosi all'apposito bancone e che possono accedere alle altre zone della sede solo se accompagnati dal personale di segreteria o da un membro del Consiglio.

Sala corsi. L'accesso è consentito ai docenti ed ai discenti dei corsi, che possono accedere alle altre zone della sede solo se accompagnati dal personale di segreteria o da un membro del Consiglio.

5. POSTAZIONI DI LAVORO

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

6. MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.
Gli archivi di documenti e atti contenenti dati sensibili dovranno essere custoditi in armadi chiusi a chiave.
L'**eliminazione fisica** di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti.
Si raccomanda di non lasciare documenti incustoditi presso i **dispositivi di stampa**.

7. GESTIONE DEI DATI PERSONALI E AZIENDALI

Ogni Utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.
I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.
È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.
È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.
Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

8. STRUMENTI INFORMATICI

L'utilizzo degli strumenti informatici in dotazione è di carattere professionale. In deroga a tale principio l'Ordine autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio dello strumento affidato utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.
Tutti gli strumenti dovranno essere bloccati e protetti da password, se lasciati incustoditi.
Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze di ricerca.
Sui dispositivi della rete dell'Ordine, non è consentito modificare in alcun modo il sistema operativo o le applicazioni installate dagli Amministratori di Sistema che rispettano le misure idonee di sicurezza.

9. POSSIBILITA' DI GESTIONE AUTONOMA DEGLI STRUMENTI INFORMATICI DI PROPRIETA' DELL'ORDINE

L'Utente, al momento della scelta di questa particolare modalità di utilizzo, dovrà sottoscrivere un documento in cui viene designato "Responsabile della gestione autonoma di strumenti informatici di proprietà dell'Ordine", tale figura deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato e dei dati di cui l'Ordine è Titolare. Per tali soggetti responsabili è prevista una attività propedeutica e periodica di formazione, come previsto dalle leggi vigenti, con il fine ultimo di fornire concetti di base riguardanti le misure adeguate di sicurezza ed i generali obblighi previsti dalla normativa vigente in materia di Privacy.

10. CUSTODIA DEGLI STRUMENTI INFORMATICI

Gli strumenti informatici di proprietà dell'Ordine devono essere custoditi dall'Utente con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.
In caso di furto o danneggiamento di beni, l'Utente dovrà informare immediatamente il Servizio IT, Infrastrutture e Patrimonio, presentare formale denuncia alle autorità di pubblica sicurezza e consegnarne copia al Servizio sopra menzionato per l'attivazione degli atti formali di scarico e di attivazione delle coperture assicurative.

11. GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate dal tecnico informatico esterno, consistono in un codice per l'identificazione dell'Utente (username), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata. Ogni Utente è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.

Sulla base della normativa vigente, le password degli Utenti devono essere cambiate almeno ogni sei mesi. Le password degli Incaricati del trattamento di dati sensibili devono essere cambiate almeno ogni tre mesi. Le password con privilegi di alto livello (root, administrator, sa, ecc.) devono essere cambiate almeno ogni tre mesi. Fanno eccezione le password che sono state preventivamente autorizzate per soli scopi di gestione tecnica il cui utilizzo assume generalmente caratteristiche di sporadicità.

12. GESTIONE E PROTEZIONE DEI DATI

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.
I dischi di rete presenti sul server dell'Ordine sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale incaricato.
Si ricorda che i dischi o altre unità di memorizzazione locali sono soggette a salvataggio automatico su apposita unità di backup.
Il personale incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che reputerà pericolosa per la sicurezza sia sugli strumenti informatici degli Utenti, sia sulle unità di rete: di tale intervento ne è informato l'Utente e il suo diretto Responsabile.
Fermi restando i vincoli esistenti a tutela della privacy per il proprio personale, gli Utenti devono essere consapevoli che i dati da loro trattati sui sistemi informatici dell'Ordine possono essere di proprietà dell'Ordine o comunque sotto la responsabilità della stessa. Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici dell'Ordine, non è possibile garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni.
La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati.
È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi di ***cloud pubblica*** non autorizzati dagli Amministratori di Sistema.

13. GESTIONE DELLA POSTA ELETTRONICA

L'assegnazione di una casella di posta elettronica dell'Ordine (da ora "e-mail Ordine") è di carattere professionale. In deroga a tale principio ORDINE autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio della risorsa affidata utilizzato a fini "privati" dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.
L'Ordine, in conformità alla disciplina in materia di privacy, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

Gli Utenti dell'e-mail Ordine sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica.
In particolare, gli Utenti devono seguire le seguenti disposizioni:

- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale, salvo specifiche esigenze di ricerca;
- prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- prestare la massima attenzione ad e-mail sospette, avvisando l'Amministratore di Sistema in caso di dubbi sulla provenienza/contenuto delle stesse;
- creare una sezione denominata "Posta personale" all'interno della propria casella di posta, alla quale gli Amministratori di Sistema non potranno accedere se non per gravi motivi di sicurezza informatica.

Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'accesso alla casella di posta dell'Utente potrà essere gestita dagli Amministratori di Sistema su richiesta del Responsabile del Trattamento dell'Utente al fine di verificare il contenuto dei messaggi e ad inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
La **Posta Elettronica Certificata (PEC)** può essere utilizzata dagli Incaricati solamente per motivi professionali.

14. UTILIZZO DELLA NAVIGAZIONE INTERNET

L'accesso a Internet è fornito principalmente per scopo professionali, per accedere a informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, gli Utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. Come per la posta elettronica, l'Ordine ne autorizza un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all'attività professionale.
Il numero e la durata degli accessi a Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli compiuti dagli Amministratori di Sistema potranno avvenire mediante un sistema di analisi dei file giornale.
Gli Utenti devono seguire le seguenti regole di navigazione della rete Internet:
a. è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'Ordine;
b. è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di ricerca;
c. è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

d. è vietato utilizzare l'infrastruttura tecnologica dell'Ordine per procurarsi e diffondere materiale in violazione con le normative vigenti;
e. è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
f. è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'Utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'Utente e quindi formalmente autorizzata dagli amministratori di sistema;
g. è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

15. ACCESSO INTERNET PER UTENTI ESTERNI

È previsto un sistema per consentire l'accesso e la navigazione in Internet ad Utenti esterni. Il numero e la durata degli accessi ad Internet sono costantemente registrati.

16. ACCESSO DA REMOTO - VPN

L'accesso dall'esterno alla rete dell'Ordine è consentito esclusivamente attraverso precise modalità di connessione sicura, indicate dal tecnico esterno incaricato. Ogni altro accesso è espressamente vietato.

17. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione dell'Ordine o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.
È assolutamente vietato divulgare notizie false. È invece autorizzata la divulgazione di informazioni già rese pubbliche dall'Ordine.

18. SISTEMI DI MONITORAGGIO RETE AZIENDALE

Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, per il tramite degli Amministratori di Sistema e nel rispetto della normativa sulla privacy, accedere direttamente a tutti gli strumenti informatici dell'Ordine.
Periodicamente e in presenza di anomalie, gli Amministratori di Sistema effettueranno verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti agli Utenti della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
Gli Amministratori di Sistema effettuano inoltre forme di controllo di carattere impersonale sulla rete e su tutti i dispositivi che la compongono. I dettagli relativi ai controlli effettuati sono disponibili nell'Appendice A.
In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.
L'Ordine è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.

19. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale deve essere utilizzata esclusivamente dal proprietario della firma.

20. SPECIFICI DIVIETI

Di seguito sono riportati specifici divieti per gli Utenti:

a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
e. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
f. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
g. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
h. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
i. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
j. caricare programmi non provenienti da una fonte certa e autorizzata dall'Ordine;
k. acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
l. detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);
m. installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;

n. utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
o. utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
p. distribuire il software aziendale a soggetti terzi;
q. realizzare codice software che violi copyright di terzi;
r. accedere illegalmente e duplicare banche dati.

21. PERDITA DELLE CONDIZIONI DI INCARICATO

In caso di perdita delle condizioni di Incaricato al Trattamento o di cessazione del rapporto con ORDINE, valgono le seguenti regole operative:
a. Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.
b. È facoltà dell'Ordine effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di Utenti non più appartenenti all'organizzazione. Le e-mail nella "Posta personale" saranno, al contrario, cancellate.
Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.
Con il dovuto anticipo, l'Utente è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con l'Ordine e - se del caso - per proporre un contatto interno alternativo.

22. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, l'Utente può rivolgersi al DPO per ricevere le opportune istruzioni.

23. RESPONSABILITÀ E SANZIONI

È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione del presente Regolamento è perseguibile nei confronti dell'Utente con provvedimenti disciplinari e risarcitori previsti dal vigente Codice Disciplinare dell'Ordine, nonché con tutte le azioni civili e penali consentite.
Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

24. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate agli Utenti e rese pubbliche sul sito internet dell'Ordine

Letto ed approvato il 05/09/18

Il Presidente Ing. Monica Boccaccio	il DPO ing. Nicoletta Rispoli

Allegato 1 - Modello Organizzativo Privacy

Regolamento Privacy dell'Ordine degli ingegneri della provincia di Alessandria

Appendice A

Dettagli relativi alle attività di controllo svolte dagli Amministratori di Sistema

L'Ordine gestisce i sistemi informatici e le reti anche attraverso strumenti che possono memorizzare temporaneamente dati relativi alla navigazione internet e al traffico telematico. In particolare si elencano:

1. Posta Elettronica - dati conservati:
a. log del traffico SMTP generato dai server di posta elettronica;
b. log dei messaggi non correttamente inoltrati (ritardi e/o mancate consegne);
c. log dei messaggi intercettati dal sistema antivirus.

2. Traffico IP – corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza:
a. Log del traffico IP generato dai dispositivi informatici.
Tale log comprende anche dati puntuali di navigazione riferibili all'indirizzo IP interno di provenienza della richiesta. I dati sono conservati per circa 26 settimane in un sistema accessibile solo dagli amministratori di sistema autorizzati, e non utilizzato normalmente per altre attività dell'Ordine. Tuttavia potranno essere conservati per tempi superiori per giustificate ragioni tecnico/organizzative, per garantire l'esercizio o la difesa di un diritto in sede giudiziarie e in tutti i casi in cui sia richiesto dall'autorità giudiziaria.

3. Telefonia – corretto funzionamento del sistema:
a. Log delle chiamate (numero chiamante, numero chiamato, durata).

4. Accesso alle reti - corretto funzionamento del sistema, monitoraggio SLA e controlli di sicurezza:
a. Log di accesso alle reti dall'esterno e dall'interno.
Come indicato nelle Linee Guida del Garante per posta elettronica e internet, l'Ordine non procederà in nessun caso a controlli non consentiti, quali:
- lettura e registrazione puntuale di messaggi di posta;
- riproduzione e memorizzazione delle pagine internet visitate;
- cattura dei caratteri digitati attraverso tastiera (fisica o virtuale);
- analisi occulta dei pc affidati in uso.