ordine degli
Architetti
Pianificatori
Paesaggisti
Conservatori
della provincia di
Perugia

REGOLAMENTO AZIENDALE INTERNO IN CONFORMITÀ AGLI OBBLIGHI DI LEGGE PREVISTI DAL NUOVO CODICE IN MATERIA DI DATI PERSONALI

APPROVATO NELLA SEDUTA DI CONSIGLIO DELL'ORDINE DEL 07.09.2023

- **Informativa e consenso**

  Nei casi in cui l'organizzazione abbia disposto la necessità di acquisire dati personali o particolari ("sensibili") attraverso l'uso di informativa e consenso, al dipendente è fatto obbligo di utilizzare la modulistica predisposta, facendola sottoscrivere dall'interessato, ove necessario.

- **Utilizzo strumentazione**

In caso di allontanamento dalla propria postazione hardware, è fatto obbligo al dipendente di spegnere il computer o di bloccarlo in modo tale che richieda la password per potervi di nuovo accedere.

- **Accesso e uso dei sistemi**

1. Il dipendente si connette alla rete tramite autenticazione univoca personale, gestisce in autonomia e ha responsabilità delle proprie password. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.

   I requisiti minimi di complessità delle password:

   a. Lunghezza di almeno otto caratteri;
   b. Redazione con caratteri maiuscoli e/o minuscoli;
   c. Possono essere inclusi simboli, numeri, punteggiatura e lettere;
   d. Non deve trattarsi di password basate su informazioni personali,

riferimenti familiari, o comunque dati inerenti il soggetto titolare della password stessa;

e. Il titolare del trattamento o l'amministratore di sistema della propria sede operativa, deve consegnare ad ogni incaricato la password contenuta in una busta chiusa. Ogni incaricato dovrà modificare tale password al primo utilizzo, e dovrà affidare una copia della propria password in busta chiusa al titolare del trattamento o l'amministratore di sistema che provvederà a custodirla in maniera riservata.

2. Il Titolare della password è tenuto inoltre a non rivelare ad alcuno, colleghi e superiori inclusi, la password, dovendone avere la massima diligenza e preservandone la segretezza anche durante il momento della digitazione.

- **Installazione programmi**
  1. Sul pc in uso non devono essere installati dal collaboratore programmi che non siano ufficialmente forniti dalla Società o dei quali non sia, espressamente e per iscritto, autorizzata l'installazione da parte del titolare dei trattamenti o dell'amministratore di sistema.

- **Utilizzo supporti magnetici**
  1. E' fatto obbligo di conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.
  2. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato su pc in uso dal collaboratore.
  3. E' fatto divieto al collaboratore di prelevare qualsiasi informazione dagli apparati dell'azienda per trasferirli su apparati personali.
  4. Ogni dispositivo di memorizzazione di massa deve preventivamente essere approvato dal titolare del trattamento o dall'amministratore di sistema.

- **Utilizzo rete interna**
  1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra i collaboratori che prestano servizio all'interno dell'azienda, non può essere utilizzata per scopi diversi da quelli ai quali è destinata, senza espressa autorizzazione della società.

2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun collaboratore preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad avere notizia di tali dati.
3. L'eventuale accesso alla rete interna wireless (quando attiva) dovrà essere preventivamente autorizzata dal titolare del trattamento o dall'amministratore di sistema.
4. L'accesso via VPN sarà preventivamente autorizzato dal titolare del trattamento o dall'amministratore di sistema e potrà avvenire solo con dispositivi mobili forniti dall'organizzazione.

- **Utilizzo rete esterna Internet e di posta elettronica**
  1. E' vietato l'utilizzo di navigazione in internet, l'uso di posta elettronica e il download di programmi per scopo personale, salvo particolare autorizzazione dal parte del titolare del trattamento o dell'amministratore di sistema.

  2. E' vietato divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio della posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti tutti i collaboratori in ottemperanza agli obblighi di fedeltà e correttezza.

  3. In caso di E-mail in cui siano presenti dei collegamenti ipertestuali ad internet si deve essere assolutamente certi del mittente e del motivo per cui è presente il collegamento, altrimenti è necessario farsi autorizzare dal titolare del trattamento o dall'amministratore di sistema.

- **Utilizzo delle Stampanti di rete**
  1. Si raccomanda di non lasciare documenti incustoditi presso le postazioni di lavoro dello scanner all'atto della scansione.
  2. Si raccomanda di non lasciare documenti nella coda di stampa del PC e di non lasciare le stampe sulle stampanti una volta completate le stampe.

- **Custodia, conservazione e controllo documenti cartacei**

1. E’ obbligatorio custodire il materiale cartaceo affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo.
2. E’ vietato lasciare qualsiasi documento incustodito presso la propria postazione qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi.
3. E’ vietato lasciare qualsiasi documento in locali estranei alla propria postazione, salvo se espressamente autorizzati, prestando particolare attenzione a non lasciarli presso la fotocopiatrice.
4. Fare particolarmente attenzione all’invio delle code di stampa quando non si è in sede con il notebook in quanto poi al collegamento queste vengono automaticamente inviate senza preavviso e la documentazione può rimanere sulla stampante.
5. E’ obbligatorio procedere con la distruzione della documentazione cartacea non più utile ai processi aziendali utilizzando:
    a. I dispositivi (distruggi documenti) posti a disposizione dalla Organizzazione;
    b. Ove la mole di documenti sia eccessiva per la struttura interna dell’Organizzazione conferire specifico incarico a società specializzata che dovrà rilasciare relativo certificato di avvenuta distruzione.

- **Violazione dei dati**

1. Per violazione dei dati si intende qualsiasi 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.

2. In caso di violazione dei dati, è fatto obbligo a chiunque ne venga a conoscenza, di darne immediata e tempestiva comunicazione in qualsiasi forma al titolare del trattamento.

- **Segreto professionale**

1. Il collaboratore non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni

apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dall'Azienda, né potrà usarle o disporne in proprio o tramite terzi. Nella valutazione delle informazioni, il collaboratore si impegna a prendere ogni misura affinché le stesse rimangano segrete, essendo inteso che, in caso di divulgazione non autorizzata dalla Società, sarà a carico del dipendente l'onere della prova di aver adottato tali misure.

2. Il collaboratore si impegna a rispettare con esattezza i suddetti obblighi perché la violazione degli obblighi contenuti in questo regolamento possono provocare ingenti danni alla Società.
3. Gli obblighi del collaboratore non termineranno all'atto della cessazione del rapporto di collaborazione, se non in riferimento a quelle specifiche parti delle informazioni che il collaboratore possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito a fatto a lui non imputabile.

- **Riservatezza dei dati**
  1. Premesso che per "informazioni riservate" si intendono tutte le informazioni di qualsiasi natura riferite o apprese durante lo svolgimento del proprio lavoro di collaborazione, il collaboratore si impegna a considerare tali informazioni come strettamente private e ad adottare tutte le misure necessarie per non pregiudicarne la riservatezza;
  2. Il collaboratore si impegna ad utilizzare le informazioni riservate per il corretto svolgimento dell'attività cui è preposto e di utilizzare tali informazioni in modo tale da non recare danno alla Società;
  3. Gli impegni previsti in questa sezione non sono da adottare qualora la comunicazione delle informazioni riservate viene effettuata:
     a. ad amministratori e collaboratori/dipendenti, anche di altre società (controllanti, outsourcing, consulenti) alle quali la conoscenza di tali informazioni è necessaria al fine dell'espletamento di attività funzionali della Società;
     b. a soggetti diversi da quelli specificati precedentemente, qualora ciò sia stato autorizzato dal titolare del trattamento o dall'amministratore di sistema.
  4. L'obbligo di riservatezza non opera in caso di informazioni riservate:
     a. che al momento in cui vengono rese note siano di pubblico dominio;

b. che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente;

5. L'impegno di riservatezza di cui alla presente sezione, si protrarrà anche dopo la cessazione del rapporto di collaborazione sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.
6. L'eventuale dismissione e/o distruzione di asset o attrezzature aziendali, per obsolescenza o altro, dovrà essere comunicata per iscritto al Titolare del Trattamento e all'Amministratore di Sistema che provvederanno ad attivare la relativa procedura (RAEE e/o quanto altro).
7. Quando gli atti e i documenti contenenti categorie particolari di dati personali e dati personali relativi a condanne penali e reati ex artt. 9 e 10 del Regolamento UE 2016/679, sono affidati agli autorizzati al trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti saranno controllati e custoditi dagli autorizzati medesimi fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

- **Attività ispettiva e sanzioni**

1. Si precisa che i sistemi informatici aziendali sono predisposti di garanzie tecniche di sicurezza e stabilità del sistema. Tali dispositivi (asset) sono configurati pertanto per inviare degli alert automatici all'Amministratore di sistema ed al Titolare. Tali segnalazioni avverranno automaticamente in caso di criticità di sistema e/o di utilizzazione dello stesso non conforme agli standard previsti dal presente regolamento che necessiteranno una verifica.
2. Il Titolare del trattamento potrà procedere alla verifica del contenuto dell'account della E-mail e degli asset aziendali nei seguenti casi:
   a. sospetto di condotta fraudolenta o scorretta del dipendente;
   b. sospetto di utilizzo della E-mail e degli asset aziendali a fini personali e non aziendali;
   c. sospetto di utilizzo della E-mail e degli asset aziendali per portare dati fuori dall'Organizzazione senza autorizzazione.

   I controlli non potranno assumere carattere continuativo, né massivo e saranno specificati al dipendete, al momento del controllo, le motivazioni e le modalità di controllo.

   In nessun caso l'attività di controllo può essere indirizzata alla verifica dell'efficienza lavorativa né può essere causa di licenziamento diretto, salvo

che si riscontrino comportamenti del dipendente illeciti e/o lesivi del patrimonio e dell'immagine aziendale (v. Cass. n. 10955 del 2015, Cass. n. 26682 del 2017).

In ogni caso l'Organizzazione si potrà avvalere dei provvedimenti disciplinari previsti dal contratto collettivo nazionale di categoria.

- **Interruzione del rapporto di lavoro**

  In ogni caso di interruzione del rapporto di lavoro le E-mail e degli asset aziendali in uso al dipendente saranno recuperati e/o disattivati.

  Ogni relativa informazione di proprietà dell'Organizzazione verrà dalla stessa utilizzata per la propria attività e continuità.

  L'account del dipendente cessato (non si riferisce ad account generici ma solo ad account che riportino direttamente o indirettamente il nominativo del dipendente cessato), verrà disattivato contestualmente alla cessazione del rapporto. Alle comunicazioni in ingresso su tale utenza verrà impostata una risposta automatica che darà atto di tale cessazione ed indicherà un account aziendale alternativo per le suddette comunicazioni.

  L'organizzazione si impegna a non conservare oltre un tempo definito e ragionevole dalla data di cessazione i dati contenuti nella casella e provvederà alla loro cancellazione entro tre mesi.

- **Applicazione ed interpretazione del presente regolamento**

  1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il collaboratore può rivolgersi al titolare del trattamento o l'amministratore di sistema.

Per ricevuta consegna

Cognome	Nome	Firma

i