DISCIPLINARE PER IL TRATTAMENTO DEI DATI

Titolare del Trattamento

EDILVALORZI S.R.L.

Fraz. Mione, 43 - 38020 RUMO (TN)

MISURE DI SICUREZZA E LINEE GUIDA AZIENDALI
PER IL TRATTAMENTO DEI DATI PERSONALI

Data di consegna	Il Ricevente per accettazione	Per il Titolare del trattamento – Rappresentante Legale

1. SOMMARIO

2. SCOPO DEL DOCUMENTO E PRINCIPI GENERALI

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti. Tali informazioni possono essere considerate, ai sensi del GDPR 2016/679, **"dati personali"** quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che la nostra organizzazione adotti una serie di misure minime ed idonee per salvaguardare il trattamento di tali dati - Privacy. Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto **"informazioni riservate",** ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali la nostra organizzazione è chiamata a garantire la riservatezza. Tali dati, nell'ambito dell'attività svolta, possono essere "**dati cartacei**" ovvero informazioni su supporto cartaceo e "**dati digitali**" ovvero informazioni che vengono memorizzate o semplicemente che transitano attraverso apparecchiature digitali.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un incaricato può venire a conoscenza e di cui **deve garantire la riservatezza e la segretezza** e non solo i "dati personali" intesi a norma di legge.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e **non deve essere comunicato o diffuso a nessuno**, **se non previa autorizzazione dell'interessato,** anche una volta interrotto il rapporto lavorativo con la nostra organizzazione salvo specifica autorizzazione della Direzione. Anche tra colleghi e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta. Come per la maggioranza delle organizzazioni, la progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dai computer aziendali espone la nostra organizzazione a possibili rischi di un coinvolgimento di rilevanza sia civile, che penale, che amministrativa, creando problemi alla sicurezza e all'immagine. Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro devono sempre ispirarsi al principio di diligenza e correttezza, la nostra organizzazione ha deciso di adottare il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature informatiche aziendali.

In sintesi, il presente documento riporta le prescrizioni di sicurezza da attuare durante il trattamento dati, decise dal Titolare del trattamento dati a seguito della relativa valutazione dei rischi eseguita.
Inoltre si ricorda che il mancato rispetto di quanto riportato nel presente documento sarà considerato fatto grave e potrà prevedere l'applicazione del sistema disciplinare previsto dal contratto di lavoro.

3. GESTIONE DEL DOCUMENTO - PUBBLICAZIONE

Copia del presente documento viene consegnato a ciascun lavoratore all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività e successivamente riconsegnato, in caso di revisioni dello stesso. Particolari forme di consegna semplificate possono essere presenti ma solo ed esclusivamente per incaricati senza l'autorizzazione all'uso di sistemi informatici e con trattamenti consentiti di sola visibilità di documenti contenenti dati (es. incaricati alla sola consultazione di documenti). In quest'ultimo caso il disciplinare viene spiegato / illustrato agli stessi e ne viene data libera consultazione presso l'organizzazione in luogo sempre accessibile. Altre metodologie di consegna / informazione sul contenuto del disciplinare possono essere adottate previa indicazione delle stesse nelle rispettive lettere di incarico predisposte per gli interessati.

Come già anticipato nel capitolo precedente si ricorda che l'inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l'incaricato, per i responsabili e per l'azienda, per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

4. CAMPO DI APPLICAZIONE

Il presente Disciplinare Interno si applica a tutte le persone autorizzate al trattamento dei dati gestiti dalla nostra organizzazione. Pertanto **le disposizioni che in seguito vengono presentate per gli "incaricati" sono da intendersi applicabili tassativamente anche ad eventuali altre figure (es. collaboratori esterni) ai quali è stata concessa l'autorizzazione al trattamento dati dalla Direzione dell'organizzazione.**

Persone autorizzate – incaricati: Sono le persone fisiche (lavoratori, dipendenti) autorizzate dal Titolare del Trattamento con specifica nomina che ne regola anche le limitazioni, a compiere operazioni di Trattamento Dati.

Responsabili: I responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Il ruolo del responsabile del trattamento di cui al regolamento europeo è chiaramente riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi.

5. RIFERIMENTI NORMATIVI E DEFINIZIONI

Regolamento Europeo Privacy - Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il nuovo **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) da cui era disceso il D.Lgs. 196/2003.

GDPR - Acronimo (General Data Protection Regolation) utilizzato per indicare il Regolamento Europeo 2016/679.

Dato Personale - Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("ineressato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo

online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie di dati particolari - dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

Trattamento dei dati - Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o 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.

Contitolarità del trattamento Art. 26 – Impone ai Titolari di definire specificatamente (con atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei Titolari operanti congiuntamente.

Responsabile Trattamento Dati - È la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Il ruolo del Responsabile del Trattamento Dati è riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi. Nel GDPR vi è specifico obbligo di predisporre un contratto per la designazione di responsabilità a carico del responsabile.

Sub Responsabile Trattamento Dati - Sono soggetti che possono essere nominati Responsabili del Trattamento Dati da parte di Responsabili. In realtà, non esiste un articolo specificatamente dedicato a tali soggetti nel GDPR, tuttavia, se ne fa menzione nell' art. 28, dedicato ai Responsabili del Trattamento, dove, al secondo comma, viene stabilito che il Responsabile del Trattamento non ricorre ad un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del Trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del Trattamento informa il Titolare del Trattamento di eventuali modifiche previste riguardante l'aggiunta o la sostituzione di altri Responsabili del Trattamento, dando così al Titolare del Trattamento l'opportunità di opporsi a tali modifiche.

Incaricati al trattamento dati - Sono le persone fisiche (lavoratori, dipendenti, collaboratori) autorizzate dal Titolare del Trattamento con specifica nomina che ne regola anche le limitazioni, a compiere operazioni di Trattamento Dati.

Misure di sicurezza art. 32 GDPR - il Regolamento prevede una lista aperta e non esaustiva delle misure tali da garantire un livello di sicurezza adeguato al rischio del trattamento. Dopo il 25 maggio 2018 non potranno sussistere obblighi generalizzati di adozione di misure minime di sicurezza, la cui valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.

Responsabile della protezione dei dati DPO (Data Protection Officer) - Il Titolare del trattamento e il Responsabile del trattamento sono obbligati a designare un "Responsabile della protezione dei dati", i cui compiti sono definiti nell.art.39 GDPR, in tre casi specifici, elencati nel paragrafo 1 dell'art. 37 GDPR, e cioè: A) se il trattamento è effettuato da un'"autorità pubblica" o da un "organismo pubblico", ad eccezione delle autorità giurisdizionali

nell'esercizio delle loro funzioni; B) se le "attività principali" del Titolare o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono un "monitoraggio regolare e sistematico" degli interessati su "larga scala", oppure C) se le "attività principali" del Titolare o del Responsabile del trattamento consistono nel trattamento su "larga scala" di "categorie particolari" di dati (c.d. dati sensibili) o di dati personali relativi a condanne penali e reati (c.d. dati giudiziari).

6. MISURE DI ACCESSO AI SISTEMI INFORMATICI

Sistema di autenticazione informatica - L'amministratore di sistema provvede a consegnare a ciascun incaricato del trattamento dei dati, all'atto di presa del servizio, le proprie credenziali di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo. Ciascun incaricato è tenuto ad adottare le necessarie cautele per assicurare la segretezza della credenziale, che non dovrà essere divulgata né resa pubblica. La parola chiave dovrà essere composta da almeno otto caratteri. Essa non dovrà contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati particolari la parola chiave è modificata almeno ogni tre mesi. Le credenziali di autenticazione non utilizzate da almeno sei mesi verranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali verranno disattivate anche in caso di perdita della qualifica che consente all'incaricato l'accesso ai dati o ad una categoria di dati. Ciascun incaricato ha il dovere di non lasciare accessibile o incustodita la propria postazione di lavoro informatica, in caso di allontanamento, anche temporaneo. Ciascun incaricato deve fornire copia delle credenziali di accesso all'Amministratore di Sistema in caso di prolungata assenza o impedimento, onde assicurare la disponibilità di dati o strumenti elettronici qualora sia indispensabile ed indifferibile l'intervento, per esclusive necessità di operatività e di sicurezza del sistema.

Sistemi di autorizzazione - Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso, è utilizzato un sistema di autorizzazione particolare per l'accesso ai dati da trattare. All'inizio del trattamento il Titolare del trattamento con la collaborazione dell'Amministratore di sistema definisce il profilo di autorizzazione per ciascun incaricato, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. La definizione dei profili verrà effettuata per iscritto nella lettera di conferimento di incarico al trattamento dati. Con cadenza annuale, il Titolare del trattamento dati verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione nei confronti di ciascun incaricato, dando evidenza delle modifiche attraverso una riformulazione della relativa lettera di incarico.

Misure di sicurezza dati informatici - I dati archiviati nella rete informatica dell'organizzazione sono protetti contro il rischio di intrusione dalle seguenti misure decise e mantenute aggiornate e sotto controllo dall'Amministratore di Sistema:

- Individuazione di password principale da digitare al momento dell'accensione del computer.
- Individuazione di un archivio principale di sistema: "ARCHIVIO H" ed individuazione di due sotto archivi "LIBERO" e "RISERVATO" ad accesso rispettivamente libero e riservato solo ad alcuni utenti.
- Individuazione degli utenti che possono accedere ai sottoarchivi e designazione degli stessi con conferimento dell'incarico (lettera di incarico).
- Presenza di antivirus.

Tutti gli incaricati sono tenuti a comunicare immediatamente all'Amministratore di sistema eventuali malfunzionamenti o sospetti attacchi di virus per consentire l'adeguato controllo e l'adozione di misure correttive e preventive adeguate ed efficaci.

7. UTILIZZO DELLE POSTAZIONI PC

La postazione di lavoro con PC, presso l'organizzazione, deve essere utilizzata solo per scopi legati alla propria attività lavorativa, utilizzata in modo esclusivo dall'utente incaricato che ne ha attivato l'accesso e protetta, evitando che altri possano accedere ai dati che si sta trattando. Si precisa inoltre che l'utente incaricato ha i seguenti obblighi:

- non utilizzare presso l'organizzazione risorse informatiche private (PC, periferiche, token, ecc..);
- non installare alcun software, se non previa autorizzazione dell'Organizzazione;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, chiavette USB, ecc.);
- disattivare il salvaschermo con password;
- non archiviare nessun dato nel proprio PC. L'archiviazione dati è consentita solo sul server. Possono essere gestiti dati sul PC solo temporaneamente qualora la procedura di lavoro adottata lo richieda ma gli stessi dovranno essere archiviati su Server non appena possibile e cancellati dal PC.

8. UTILIZZO DI PC PORTATILI

Il Titolare del trattamento dati autorizza l'uso di un PC portatile dandone comunicazione all'utente sulla lettera e pertanto l'incaricato può utilizzare e collegare alla rete dell'organizzazione solo il PC portatile autorizzato. L'autorizzazione al loro utilizzo, qualora espressa, è riportata/integrata nella lettera di incarico al trattamento o nel contratto predisposto per eventuali collaboratori esterni. Quanto disposto nel capitolo "**misure di accesso ai sistemi informatici**" si applica anche ai PC portatili autorizzati e collegabili alla rete dell'organizzazione. Nella lettera di incarico o nel contratto potranno essere disposte particolari prescrizioni di trattamento dati con PC portatili da considerare "integrative" al presente disciplinare.

Non lasciare il PC portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione).

La perdita di PC portatili o eventuali danni derivanti dalla mancata osservanza di quanto disposto nel presente Disciplinare e da quanto richiesto dalla diligenza del buon padre di famiglia/ del comune buon senso saranno imputati all'incaricato.

9. USO DI CHIAVI USB O ALTRI SUPPORTI ESTERNI DI SALVATAGGIO DATI

Uso chiavette USB o altri supporti esterni amovibili di salvataggio – Data la natura del lavoro svolto **l'uso di tali supporti è consentito** anche se con particolare attenzione, moderazione e solo ed esclusivamente nei casi in cui risulta assolutamente necessario per l'esecuzione del lavoro da svolgere. Risulta comunque VIETATO archiviare su tali supporti "dati particolari" per i quali, se necessario, dovranno essere utilizzate altre forme di trasferimento come ad esempio l'e-mail.

Misure di sicurezza da adottare – Come noto i dispositivi chiavette USB o altri simili (in seguito denominati "dispositivi") sono maneggevoli e facilissimi da trasportare, ma comportano particolari rischi, per i quali presso la nostra organizzazione, sono state disposte le seguenti prescrizioni:

- Potranno essere utilizzati solo "dispositivi" consegnati all'incaricato dall'organizzazione. Non potranno pertanto essere utilizzati "dispositivi" personali/privati. I "dispositivi" saranno consegnati con una specifica lettera di consegna controfirmata sulla quale sarà registrata inoltre la data della riconsegna del "dispositivo" da parte dell'incaricato. La riconsegna deve essere eseguita a fine rapporto di lavoro o in caso di "dispositivo" difettoso o non funzionante all'Amministratore di sistema o alla Direzione dell'organizzazione o alla persona autorizzata dal Titolare del trattamento. In caso di restituzione del "dispositivo" per difettosità o rottura sarà riconsegnato all'incaricato un altro "dispositivo" sempre con lettera di consegna controfirmata. Spetta quindi all'Amministratore di sistema o alla Direzione distruggere i "dispositivi" difettosi o non funzionanti in modo tale che nessuno possa più utilizzarli. La distruzione del "dispositivo" è registrata nella lettera di consegna-riconsegna del dispositivo stesso.
- Non potranno essere consegnati "dispositivi" senza la previa restituzione del precedente e pertanto un incaricato non potra mai avere più di un "dispositivo". In caso di smarrimento del "dispositivo" l'evento sarà registrato nella lettera di consegna dello stesso dove dovrà essere registrato il giorno di smarrimento, il potenziale luogo, ed una descrizione dei dati ivi contenuti.
- E' assolutamente vietato utilizzare tali "dispositivi" per trasferire dati di lavoro (sia dell'organizzazione che di clienti o di terzi inerenti i lavori eseguiti) su dispositivi informatici privati. Tale condotta costituisce illecito penale punibile dalla legge / aspetto è configurabile come furto di dati e può essere perseguito.
- Per evitare di smarrire o dimenticare i "dispositivi" nel luogo di utilizzo in forma incustodita, devono essere utilizzati esclusivamente dispositivi dotati di fori, ganci o anelli. Il dispositivo deve essere quindi agganciato ad un oggetto (es. chiavi della macchina,…) in modo tale che la dimenticanza dello stesso non sia possibile.

- Eventuali danni derivanti dalla mancata osservanza del rispetto di quanto disposto dal presente Disciplinare saranno imputati all'incaricato.

10. MISURE DI SALVATAGGIO E RECUPERO DATI

Salvataggio dei dati informatici presenti nel Server - L'Amministratore di Sistema dispone il salvataggio dei dati:

- server gestionale completo (ARCA e Impresa) con la seguente frequenza: ogni giorno ad ore 19:00 dal lunedì al venerdì per un totale di 5 back up settimanali. Sono presenti due dischi di back up intercambiabili (A e B). A cadenza mensile viene intercambiato il disco di backup.
- archivio documenti differenziale ogni giorno ad ore 23:30 dal lunedì al venerdì e completo nella giornata di sabato sempre alle ore 23:30.
- Archivio outlook differenziale ogni giorno ad ore 20:00 dal lunedì al venerdì e completo nella giornata di domenica sempre alle ore 20:00.

Salvataggio dei dati informatici presenti sui singoli PC fissi - L'Amministratore di Sistema NON dispone alcun tipo di salvataggio dati visto il disposto divieto di archiviare sugli stessi dati - rif. Capitolo "Utilizzo delle postazioni PC". Non è consentito agli incaricati eseguire copie di salvataggio.

Salvataggio dei dati informatici presenti sui singoli PC portatili - L'Amministratore di Sistema dispone il salvataggio dei dati presenti sul PC portatile autorizzato, con la seguente frequenza: al collegamento del PC portatile alla rete dell'organizzazione si attiva un backup dati alle ore 13 di ogni giorno dal lunedì al venerdì. L'incaricato dovrà collegare il PC portatile alla rete ogni qualvolta sia presente in ufficio.

Custodia dei supporti con le copie di sicurezza - Il disco di back up del server rimosso viene conservato, sotto la tutela del Titolare del trattamento in un sito diverso da quello del Server (armadio chiuso a chiave) per evitare una potenziale distruzione di tutti i supporti in caso di calamità / incendio nel luogo di installazione del server.

Recupero dati – Con frequenza almeno mensile sono eseguite da un incaricato delle prove di recupero dati per assicurarsi del funzionamento del back up. Le prove sono registrate.

11. USO DI INTERNET

La connessione alla rete internet dal device avuto in dotazione **è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa**. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento. In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati.

Misure preventive per ridurre navigazioni illecite - L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

Divieti Espressi concernenti Internet – In seguito si riportano i divieti posti dall'organizzazione per regolamentare l'uso non corretto di internet da parte degli incaricati:

- È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.
- È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
- È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet senza specifica autorizzazione dell'Amministratore di sistema;
- È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di social network, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
- È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
- È' vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'organizzazione stessa.
- È vietato creare siti web personali sui sistemi dell'organizzazione;
- E' vietato acquistare/vendere beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale e/o dell'organizzazione.

Ogni eventuale navigazione che comporta un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati è posta sotto la personale responsabilità dell'Incaricato inadempiente.

Divieti di Sabotaggio - È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dal creatore/gestore del sito per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

Diritto d'autore - È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'organizzazione.

12. GESTIONE POSTA ELETTRONICA

La Posta Elettronica è uno strumento di lavoro - L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente se compatibile con le prescrizioni del presente disciplinare. Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica di clienti e/o terzi memorizzati nel server dell'organizzazione. Le caselle e-mail sono assegnate con natura impersonale (tipo info, amministrazione, ...) proprio per evitare che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito. Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica - L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

- In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
- Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

Divieti Espressi – In seguito si riportano i divieti imposti dalla nostra organizzazione al fine di tutelare il corretto trattamento dei dati:

È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.

- È vietato creare, archiviare o spedire, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare

a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

- È vietato trasmettere messaggi a gruppi numerosi di persone senza l'autorizzazione necessaria.
- È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
- È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione al lavoro svolto.

Posta Elettronica in caso di assenze programmate ed assenze non programmate - Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply). In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza. Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

Utilizzo Illecito di Posta Elettronica - È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

13. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Il Titolare per il trattamento dei dati personali, all'atto del conferimento, impartisce istruzioni scritte agli incaricati finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Documenti con dati personali: sono gestiti dagli incaricati e sono riposti in archivi / scaffali non dotati di particolari sistemi di chiusura/accesso controllato. Durante l'elaborazione delle pratiche non sono date particolari prescrizioni se non quelle della riservatezza e corretta conservazione.

Documenti con dati particolari: L'accesso agli archivi contenenti dati particolari è controllato con un sistema di chiusura con chiave e solo alcuni incaricati possono occuparsi degli stessi. Quando gli atti e i documenti contenenti

dati particolari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono riposti al termine delle operazioni affidate negli archivi chiusi.

14. ACCESSO DI TERZI NEL LUOGO DI TRATTAMENTO DATI

Accessi di terzi durante l'orario di lavoro ai luoghi di archiviazione dati: L'accesso di terzi presso i luoghi di archiviazione dei dati è consentito solo alla presenza di un incaricato interno al quale spetta il compito di rimuovere dallo spazio di lavoro, o più in generale di incontro, documenti contenenti dati riservati e di sorvegliare affinchè non siano rimossi deliberatamente o involontariamente dati dai terzi accolti.

Accessi di terzi dopo l'orario di chiusura - Qualora si rendesse necessario accordare l'accesso ai luoghi di lavoro e di archiviazione dati a terzi (es. vigilanti, addetti alle pulizie,…) spetta al Titolare del trattamento autorizzarne l'accesso in forma scritta previa identificazione. Nel documento di autorizzazione scritta dovranno essere indicati anche i divieti di trattamento dati o eventuali modalità di trattamento consentite in relazione all'incarico coperto dalle persone autorizzate all'accesso fuori dell'orario di lavoro. I documenti di autorizzazione all'accesso, controfirmati dalle parti, devono essere conservati dal Titolare del trattamento.

15. LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati per garantire la massima riservatezza degli stessi.

- l'Incaricato deve osservare tutto quanto disposto nel presente Disciplinare nonché tutte le regole di ordinaria diligenza;
- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate (es. Clienti, terzi che per motivi riferibili all'attività svolta possono essere presenti nei luoghi di lavoro dell'Organizzazione), che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie affinché soggetti non autorizzati non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che informatico;
- non devono essere eseguite operazioni di trattamento non correlate al proprio lavoro o esplicitamente autorizzate;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti e deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.
- non lasciare incustoditi cellulari o altri dispositivi elettronici contenenti dati;
- non utilizzare fax e/o telefono per trasmettere dati se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

16. VIDEOSORVEGLIANZA

Non Presente.