

REGISTRO DI ATTIVITA' DI TRATTAMENTO
(ART. 30 E 32 REGOLAMENTO UE 679/2016 - GDPR)

*** ** **

Per Ecostil Group Srl

responsabile del Trattamento dati: Perin Rinaldo

L'azienda Ecostil Group Srl tratta i seguenti dati:

a – dati comuni dei clienti, dipendente, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali, pubblica amministrazione e banche dati accessibili al pubblico;

b - dati comuni dei clienti dagli stessi comunicati per l'espletamento degli incarichi professionali, compresi dati sul patrimonio, dati sulla situazione economica, o necessari ai fini fiscali o attinenti alla reperibilità e alla corrispondenza con gli stessi;

c – dati comuni dei fornitori forniti dagli stessi e relativi alla reperibilità o alla corrispondenza con gli stessi, nonché inerenti a fini fiscali o di natura bancaria

d- dati comuni di dipendenti dell'azienda

La società tratta i seguenti **dati sensibili**:

a – tratta dati sensibili dei clienti/terzi/fornitori/dipendenti idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;

b – può trattare a dati di terzi forniti dai clienti/terzi/fornitori e dipendenti o acquisiti per l'espletamento degli incarichi idonei a rivelare lo stato di salute;

c – può trattare tratta dati sensibili di clienti/terzi/fornitori e dipendenti e di terzi afferenti la vita sessuale;

I dati sopradescritti vengono acquisiti previa informativa che viene allegata al presente Registro di Attività di Trattamento (art. 30) e vengono conservati in fascicoli non trasparenti riposti in schedari chiusi con chiave e posti nei locali di cui all'ufficio.

Inoltre sono contenuti nel fascicolo informatico con il programma gestionale accessibile dalla rete e protetto con password in possesso solo del titolare, e vengono archiviati al termine dell'incarico.

Il trattamento dei dati è fatto prevalentemente all'interno dell'ufficio.

I collaboratori trattano i dati solo per il tempo necessario all'espletamento di attività contabili ed amministrative.

L'ufficio ove vengono conservati i dati è dotato di citofono e portone di ingresso con apertura automatica, nonché porta ingresso e porta a vetri.

L'ufficio è dotato di n°8 computer dotati di un software gestionale, collegato con una linea telefonica con accesso alla rete internet, e vi sono stampante – fax – fotocopiatrice.

La rete informatica è costituita da sistema operativo Windows 2008 server con antivirus Virit, con la configurazione dei diritti di accesso protetta da password. Ogni stazione di lavoro Windows è dotata di software antivirus con aggiornamento automatico e firewall. L'accesso a internet avviene tramite browser ed è accessibile solo da chi ha la password del PC. Non è previsto alcun impiego di supporti di memorizzazione esterno.

Incaricato del trattamento dei dati è Rinaldo Perin titolare dell'attività e i dati comuni dei dipendenti, clienti, dei fornitori, dei terzi e di altri professionisti, sono trattati oltre che dal titolare anche dal sig. Stefano Toniazio, incaricato specificamente dal sig. Perin a tale scopo.

ANALISI DEI RISCHI

Per quanto concerne i dati comuni raccolti relativi ai soggetti specificati nella prima parte del presente documento i rischi legati alla gestione e al trattamento può definirsi basso.

Per i dati sensibili dei clienti, dei terzi dei fornitori e dei dipendenti, i rischi legati al loro trattamento possono definirsi bassi.

Per i dati sensibili riguardanti lo stato di salute, o idonei a rivelare la vita sessuale, per le pratiche riguardanti la sfera personale e familiare il rischio può definirsi medio.

I rischi relativi agli strumenti elettronici presenti in ufficio possono riguardare mal funzionamenti o guasti, eventi naturali alterazioni nella trasmissione. Per ridurre i rischi al minimo sono state adottate oltre alle misure di sicurezza sopra specificate le seguenti misure di sicurezza come password di otto caratteri sostituita ogni tre mesi scelta dal titolare.

Si è data disposizione di considerare internet e posta elettronica quali strumenti di lavoro e si è pertanto vietata la navigazione in internet su siti poco attendibili o non ufficiali e si è data disposizione di non aprire email provenienti da soggetti non conosciuti e di non inviare email non autorizzate dal titolare.

I rischi relativi ai software possono consistere in errori o virus. Si è data disposizione di provvedere periodicamente alla pulizia dei file temporanei e del disco rigido, alla deframmentazione etc.

Il rischio per il trattamento dei dati cartacei può essere considerato basso essendo l'archivio dotato di chiusura a chiave e i fascicoli riposti in armadi chiusi, fatti salvi gli eventi naturali.

E' stata data disposizione che i fascicoli contenenti i dati siano sempre riposti negli appositi schedari e prelevati per il tempo necessario al trattamento e che non vengano lasciati incustoditi sulle scrivanie, che le comunicazioni a mezzo posta o fax debbano essere smistate immediatamente ai destinatari.

E' stata data disposizione che il materiale cartaceo destinato allo smaltimento sia distrutti e riposto in sacchi di plastica non trasparenti o contenitori chiusi al fine di evitarne la fuoriuscita e smaltiti una volta alla settimana.

Per quanto riguarda il rischio per il trattamento dei dati elettronici può essere considerato basso essendo adottati tutti i sistemi di sicurezza derivanti dalla gestione dei dati.

Il rischio di perdita dei supporti di memorizzazione è basso.

Eventuali utenti saranno formati, rispettivamente per i loro ruoli, all'atto dell'ingresso nella struttura dell'ufficio e dell'installazione di nuovi sistemi, dai tecnici venditori dei sistemi stessi e, per quanto concerne le procedure per garantire le misure di sicurezza, dal titolare del trattamento. Gli incaricati dovranno comunicare immediatamente al titolare disfunzioni dei sistemi operativi e sono autorizzati a richiedere l'intervento del tecnico incaricato in caso di interruzioni e disfunzioni.

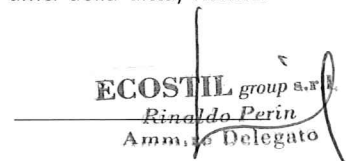
Terzi operatori tecnici interverranno sugli strumenti informatici previa autorizzazione ed invito ad effettuare gli interventi limitatamente alla prestazione da eseguire e alla presenza del titolare o delle persone autorizzate. Il rischio di accesso ai locali può essere considerato basso essendo dotato di porta d'ingresso a chiusura singola e campanello, così come l'accesso di terzi estranei all'azienda, essendo dotato di porta con chiusura ed essendo l'accesso previamente controllato da sistema di allarme con ingresso tracciabile. Il rischio che terzi estranei accedano agli strumenti elettronici è basso essendo la sala di attesa dei clienti distante dalle postazioni di lavoro.

La società ha provveduto ad adottare le disposizioni sulla sicurezza. I rischi eventuali sono inerenti ad eventi naturali e accidentali. Il rischio può essere considerato basso.

I dati trattati dall'azienda non possono essere considerati di interesse per eventuali terzi.

Il presente documento è stato redatto in duplice originale e conservato firmato negli uffici della ditta, nonchè inviato a mezzo pec ecostilgroup@legalmail.it data 18/05/2018.

Vicenza, 18/05/2018


ECOSTIL group s.r.l.
Rinaldo Perin
Amministratore Delegato