Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

REGOLAMENTO PROCEDURE PRIVACY – SOMEL IMPIANTI SRL

Il presente Regolamento interno aziendale dispone le procedure che tutti i lavoratori della Società (di seguito "Azienda") devono adottare nel rispetto del nuovo Regolamento Europeo (GDPR) inerente la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

All'interno del nostro Regolamento sono indicate anche le informazioni principali relative alla normativa europea applicata al nostro contesto aziendale, nonché le principali definizioni di legge.

PRINCIPI GENERALI

La nostra Azienda è tenuta a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

In particolare, il trattamento dei dati deve rispettare i seguenti principi:

- di liceità: conformemente alle disposizioni del Regolamento (il trattamento è necessario per: l'esecuzione di un contratto di cui l'interessato è parte, per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso; per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento; per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento; per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o diritti e libertà fondamentali dell'interessato. Nel caso in cui l'interessato ha espresso il consenso al trattamento dei propri dati per una o più specifiche finalità), nonché alle disposizioni del Codice Civile, (il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume);
- di correttezza;
- di trasparenza: consentendo all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- di adeguatezza: deve essere riferibile alla tipologia di incarico o mansione svolta;
- di pertinenza: i dati devono essere trattati in relazione allo scopo cui sono destinati;
- della limitazione: la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita;
- di esattezza: i dati devono essere esatti ed aggiornati;
- di integrità: adottando misure tecniche ed organizzative idonee di protezione;
- di riservatezza: impedendone la divulgazione a soggetti non autorizzati.

OBBLIGHI DI SICUREZZA

La nostra Azienda è tenuta a garantire che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base allo stato dell'arte e all'avanzamento tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

MISURE DI SICUREZZA IDONEE

La nostra Azienda è tenuta ad adottare un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza per assicurare un livello idoneo di protezione dei dati personali sia nel caso di trattamenti con strumenti elettronici che per trattamenti senza l'ausilio di strumenti elettronici.

DATI GENERALI

Titolare del trattamento: SOCIETA' SOMEL IMPIANTI SRL

Finalità del trattamento:

Gestione del rapporto contrattuale con il cliente

Gestione del rapporto contrattuale con utenti di servizi o fornitori di beni

Comunicazione con clienti, fornitori, soci, amministratori, terzi, alla corrispondenza con gli stessi o richiesti a fini fiscali

Gestione del rapporto di lavoro con i dipendenti e collaboratori, ai fini contrattuali, previdenziali, assicurativi e fiscali

Attività inerenti gli adempimenti fiscali o contabili

Svolgimento della propria attività

Tutela del legittimo interesse del Titolare

Tipologia di dati Trattati

I dati personali trattati sono: anagrafici, amministrativi, contabili, bancari, fiscali, contatti di vario genere, documenti identificativi.

Dati particolari: inerenti lo stato di salute, ed eventualmente a condanne (per i lavoratori dipendenti).

TRATTAMENTI AFFIDATI ALL'ESTERNO

Il Titolare del trattamento, relativamente ad alcuni trattamenti di dati, ha affidato la loro gestione a soggetti esterni designandoli formalmente con apposita lettera di nomina in qualità di Responsabili del Trattamento Esterno.

Il trattamento di dati avviene ai soli fini dell'espletamento dell'incarico ricevuto, nel rispetto degli obblighi previsti dal Regolamento per la protezione dei dati personali, nonché nel rispetto delle istruzioni specifiche ricevute dal Titolare del trattamento.

I nominativi dei Responsabili del Trattamento, i dati trasferiti, nonché le relative finalità, sono contenute all'interno del "Registro delle attività di trattamento" redatto e mantenuto aggiornato a cura del Titolare del Trattamento e conservato nei propri archivi amministrativi.

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

PROCEDURE PER L'ACCESSO, LA CONSERVAZIONE E LA CANCELLAZIONE DEI DATI

Tutti i dati trattati all'interno dell'Azienda sono accessibili al solo personale debitamente formato e nominato con apposita lettera di nomina.

Viene consentito agli interessati di accedere ai propri dati per:

verificarne la veridicità; aggiornarli; integrarli; richiederne la cancellazione (ove non pregiudichi il perseguimento delle finalità del trattamento).

La conservazione dei dati può avvenire con modalità informatiche o cartacee, a seconda delle finalità e dell'organizzazione interna, per un arco temporale non superiore al conseguimento delle finalità per le quali sono stati raccolti.

I dati strettamente necessari per gli adempimenti fiscali, contabili e per la gestione del rapporto di lavoro, venuta meno la finalità per la quale erano stati raccolti, verranno comunque conservati per un periodo non superiore a 10 anni e comunque secondo disposizioni di cui all'art. 22 del DPR n. 600/1973 (Tenuta e conservazione delle scritture contabili).

In osservanza al corrispondente diritto di accesso all'interessato, gli interessati possono richiedere la cancellazione senza ingiustificato ritardo dei dati personali o limitazione del trattamento dei dati personali quando:

i dati non sono più necessari per la finalità per i quali erano stati raccolti; l'interessato ha revocato il consenso al trattamento dei dati (quando previsto); l'interessato si oppone al trattamento; i dati sono trattati illecitamente.

MISURE DI SICUREZZA IDONEE ADOTTATE AL LIVELLO CARTACEO

L'accesso all'archivio degli atti e dei documenti contenente dati personali è consentito al solo personale autorizzato e debitamente formato.

L'archivio dei dati è ubicato negli uffici amministrativi a cui può accedere il solo personale autorizzato, nonché soggetti esterni se accompagnati da soggetti autorizzati.

Documenti che contengano dati sensibili od eventualmente giudiziari sono conservati in locale con porta blindata e/o armadi chiusi a chiave.

Gli atti e i documenti quando sono prelevati per essere utilizzati devono essere riposti in archivio prima dell'orario di chiusura.

Non sono ammesse persone dopo l'orario di chiusura se non espressamente autorizzate dal titolare.

MISURE DI SICUREZZA IDONEE ADOTTATE A LIVELLO ELETTRONICO E CARTACEO

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

L'operatore può accedere ai computer ai quali è autorizzato esclusivamente inserendo le proprie credenziali e la propria password. L'addetto non può diminuire il livello di sicurezza stabilito dall'amministratore di sistema per il computer a cui accede. Per prevenire l'accesso ai dati da parte di operatori non autenticati l'addetto che si allontani dal proprio dispositivo ricevuto in dotazione aziendale (Personal Computer, Tablet, I Phone, portatile) anche solo per pochi minuti, deve impostare il blocco del dispositivo secondo la procedura del sistema operativo utilizzato (Windows, Mac, Android, ecc.) e comunque con le modalità ritenute più idonee.

L'addetto deve operare con diligenza ponendo estrema cura ed attenzione nell'utilizzo del computer e delle applicazioni al fine di evitare cancellazioni e modifiche errate, accidentali o intenzionali che possano arrecare danno o pregiudizio alla nostra organizzazione e per le quali sarà ritenuto responsabile.

L'addetto deve segnalare immediatamente al diretto superiore eventuali anomalie di funzionamento dei computer e delle eventuali applicazioni utilizzate.

Sistema di Autenticazione

L'utente ricorda la propria username e la propria password che sono memorizzate sul sistema di accesso. Per la scelta della password, di seguito sono indicate le “Linee guida per la scelta della password”.

In caso di trattamento di dati sensibili conservati su sistemi informatici, la parola chiave deve essere cambiata almeno ogni tre mesi o quando si può avere il dubbio che la password sia conosciuta da terzi.

Protezione da accessi non consentiti

Nel caso di accessi non autorizzati verranno immediatamente bloccate tutte le operazioni sui computer e verrà contattato immediatamente il Consulente Informatico che dovrà disattiverà momentaneamente tutte le connessioni con internet e controllerà i computer, tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi e per il ripristino della normalità. Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti o di sabotaggio si provvederà all'immediata denuncia presso le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati. Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione, ma comunque non a scopo fraudolento o di sabotaggio verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori delle norme sindacali, dalle norme deontologiche.

Protezione da trattamenti illeciti dei dati

I dati sono protetti da un sistema di autenticazione che concede l'accesso agli addetti autenticati attraverso il riconoscimento di password d'accesso ai dati. Nel caso di carenza di consapevolezza, disattenzione o incuria degli addetti sarà bloccato temporaneamente l'accesso ai dati degli addetti e nuovamente formato l'addetto sulle procedure del trattamento. Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti ed adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

Protezione da programmi informatici

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

Su ogni PC è attivo un software antivirus con frequenza automatica. Nel caso di azione di virus informatici verranno immediatamente bloccate tutte le operazioni su tutti i computer attraverso l'utilizzo di un programma antivirus aggiornato e verranno immediatamente verificati e bonificati tutti i computer infetti. Nel caso di spamming verranno immediatamente bloccate tutte le operazioni su tutti i computer e il Consulente Informatico disattiverà momentaneamente tutte le connessioni con Internet, verificherà i firmali su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer. Nel caso di azione dei programmi suscettibili di recare danno verranno immediatamente bloccate tutte le operazioni su tutti i computer e il Consulente Informatico disattiverà i programmi dannosi e verranno immediatamente verificati e bonificati i computer.

Procedure di backup

Le copie di backup vengono effettuate:

- automaticamente con frequenza giornaliera su disco esterno.

Procedure per la custodia delle copie di sicurezza

Le copie di backup dei dati sono conservate:

- SU SUPPORTO DIGITALE PRESSO LA SEDE LEGALE DELLA SOCIETA'
- SU CLOUD GOOGLE DRIVE

Le copie di backup sono accessibili esclusivamente ad operatori autorizzati.

Misure di sicurezza da adottare, in caso di utilizzo di strumenti informatizzati portatili (Smartphone, tablet, PC Portatili):

- Utilizzare sempre il codice identificativo personale e le parole chiave. La password dovrà essere modificata ogni 6 mesi e comunque ogni qual volta venga percepito o rilevato un rischio alla sicurezza della medesima; laddove possibile, utilizzare sempre almeno 8 caratteri, mescolando caratteri maiuscoli, minuscoli e simboli.
- Evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.
- Accertarsi di effettuare con frequenza la copia di backup dei dati archiviati sul personal computer o supporto di memoria asportabile. Si faccia attenzione a che le modalità di custodia di questi supporti portatili siano effettuate con la massima attenzione in modo da evitarne la perdita.
- Non tenere mai insieme le copie di backup ed il personal computer, per evitare che un eventuale furto possa coinvolgere sia i dati del personal computer che quelli di backup.
- Se durante la giornata vi spostate molto dalla vostra postazione o durante la notte lasciate il vostro portatile in ufficio, riponetelo in armadio chiuso a chiave.
- Tutte le precauzioni che vengono prese all'interno dell'azienda per filtrare virus e messaggi di posta elettronica non autorizzati potrebbero non essere attive quando il personal computer viene collegato ad una presa telefonica di un albergo o comunque di locali esterni. Si faccia quindi particolare attenzione, quando ci si collega ad Internet attraverso reti non dotate di appropriati filtri, al tipo di messaggio che viene ricevuto.
- Ci si accerti che il software antivirus, presente sul personal computer, sia costantemente aggiornato o ci si accerti che il sistema operativo ed altri applicativi residenti siano sempre aggiornati e che il firewall, se presente, abbia un profilo di attività aggiornato.
- Quando ci si collega ad Internet, la prima operazione da fare è sempre quella di aggiornare il software antivirus, software di base ed i software applicativi residenti; successivamente procedere con altre operazioni.

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

- Se scopriste che il vostro personal computer è infetto da virus, chiedete subito istruzioni al Consulente Informatico sugli interventi da attuare e non effettuate ulteriori elaborazioni.
- Collegatevi regolarmente al sito Internet del venditore degli applicativi residenti su personal computer, in modo da avere sempre a disposizione gli ultimi aggiornamenti, che molto spesso sono mirati a migliorarne la sicurezza.
- Non lasciate mai il personal computer collegato ad Internet senza il vostro presidio; cercate di tenervi collegati soltanto per il minimo tempo necessario per effettuare le operazioni desiderate.
- Non permettete ad alcuna persona, anche di fiducia di accedere al vostro personal computer.
- Se avete necessità di gestire dati riservati su un portatile, installare un programma di cifratura del disco rigido.

Istruzioni generali al trattamento di dati con strumenti elettronici e con modalità cartacee

Il termine "sicurezza" si riferisce a tre aspetti distinti:

- Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni.
- Integrità: Le informazioni non devono essere alterabili da incidenti o abusi.
- Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi in quanto le misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, ma nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Solo i soggetti autorizzati dall'Azienda possono accedere all'archivio informatico e cartaceo aziendale; tali soggetti devono rispettare le regole sotto indicate:

- Chiudere a chiave (ove presenti) le porte dell'ufficio e riporre i documenti al loro posto in appositi contenitori.
- Conservare i documenti in luoghi sicuri: tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo non riconducibile direttamente ai nominativi dei clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche.
  Tutti i contenitori con i documenti (non contenenti dati sensibili) possono essere posti in scaffalature a giorno se l'accesso ai locali avviene solo da parte di personale autorizzato al trattamento dei dati; se i documenti riguardano dati sensibili o giudiziari oppure luoghi in cui può avvenire l'accesso da parte di persone non autorizzate al trattamento, devono essere riposti in armadi con serratura o ripostigli con porte con serratura. Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati; riponeteli sempre nei loro contenitori.

- Conservare i supporti informatici esterni (quali USB, memorie esterne, CD, …) in un luogo sicuro. Riponeteli quindi sotto chiave in armadi o archivi non appena avete finito di usarli. Proteggete l'accesso delle pen-drive con una password. Non tenere le copie di backup delle memorie esterne vicino al computer.
- Utilizzate le password. Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
  - la password di accesso al computer che impedisce l'utilizzo improprio della vostra postazione quando per un motivo qualsiasi non vi trovate in ufficio;

- la password di programmi specifici (se presenti) che impedisce l'accesso ai documenti realizzati con quelle applicazioni;
- la password del salvaschermo che impedisce in caso di una vostra assenza momentanea a persona non autorizzata di visualizzare il vostro lavoro.

L'utilizzo di questi tipi fondamentali di password è obbligatorio.

- Non lasciate accedere ai documenti elaborati da stampanti o fax da parte di persone non autorizzate. Recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe contenenti dati personali o particolari quando non servono più. Nel caso di documenti contenenti dati sensibili o giudiziari utilizzate la macchina distruggi documenti (se presente).
- Non fatevi spiare quando state digitando la password: anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete una buona capacità di digitazione.
- Custodite la password in un luogo sicuro: se lo ritenete necessario, scrivete la vostra password, chiudetela in busta chiusa e consegnatela al Titolare del Trattamento che la conserverà in armadio chiuso a chiave.
- È fatto divieto far usare il vostro computer a personale esterno non autorizzato.
- È fatto divieto collegare supporti elettronici esterni non autorizzati ed installate programmi non autorizzati.
- Adottate con cura le linee guida per la prevenzione di virus sotto riportate.
- Controllate che i back up effettuati avvengano correttamente.
- Segnalate qualunque anomalia al diretto superiore ed eventualmente direttamente al Consulente Informatico: anomalie sia nelle funzionalità del singolo computer, sia su qualsiasi altra applicazione che state utilizzando.

Linee guida per la prevenzione dei Virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Un virus può trasmettersi:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le email ricevute;
- attraverso il download da Internet.

Come NON si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpeg, ecc);
- attraverso email non contenenti allegati.

Il virus è estremamente pericoloso quando:

- si installano programmi;
- si copiano dati, dai dischetti;
- si scaricano dati o programmi da internet.

Il virus può avere i seguenti effetti:

- Effetti sonori e messaggi sconosciuti appaiono sul video.
- Nel menù appaiono funzioni extra finora non disponibili.
- Lo spazio sul disco si riduce inspiegabilmente.

- Le funzionalità dei computer rallentano repentinamente.

Come prevenire i Virus:

- Usate soltanto programmi provenienti da fonti fidate: copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. È fatto divieto installare ed utilizzare programmi non autorizzati dall'Azienda.
- Assicuratevi di non far partire accidentalmente il vostro computer da dischetto, Cd o DVD: infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
- Assicuratevi che il vostro software antivirus sia aggiornato: è obbligatorio che il programma antivirus sia aggiornato periodicamente (non oltre sei mesi).
- Assicuratevi che sul vostro computer sia attivato il Firewall: verificate dalle preferenze del vostro computer o chiedete al diretto superiore o al Consulente Informatico;
- Non diffondete messaggi di provenienza dubbia.
- Non aprite allegati alle email inviate da sconosciuti o da mittenti la cui provenienza non sia certa.

Linee guida per la scelta della password

La scelta di password "sicure" è parte essenziale della sicurezza informatica.

Caratteristiche della password:

- Deve avere almeno 8 caratteri alfanumerici, con maiuscole e minuscole, e simboli.
- Deve essere preferibilmente priva di significato e non deve essere comunicata a soggetti terzi, anche se fiduciari, né riconducibile all'utilizzatore (es: nome di figli, animali domestici, ecc..).
- Utilizzate password distinte per l'accesso avari sistemi.

È vietato:

- scrivere la password su appunti accessibili da parte di soggetti non autorizzati, soprattutto vicino al computer.

È obbligatorio:

- Cambiare la password a intervalli regolari. Se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni 3 mesi, altrimenti ogni sei mesi.

AZIONI DA ATTIVARE IN CASO DI EVENTI DANNOSI

Nell'ottica dell'importanza della circolazione dei dati e della correlata necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere a porre in essere azioni al seguito del verificarsi di eventuali eventi dannosi o pericolosi per il trattamento dei dati personali.

In relazione alle possibili intromissioni o effrazioni ai sistemi informatici (attacco di un virus, hackeraggio, furto dati,….) devono essere associate le relative azioni correttive.

- Nel caso di accessi non autorizzati:
  verranno immediatamente bloccate tutte le operazioni su tutti i computer ed il Consulente Informatico disattiverà momentaneamente tutte le connessioni con Internet;

verranno controllati tutti i computer, tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi non autorizzati e per il ripristino della normalità.

Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti, o di sabotaggio si provvederà all'immediata denuncia pressò le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.

Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione, ma comunque non a scopo fraudolento o di sabotaggio verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

In ogni caso per ognuna delle situazioni sopra citate o comunque per tutte le violazioni dei dati si provvederà a dare tempestiva comunicazione all'autorità garante.

Per accesso non autorizzato si intende:

l'accesso effettuato da un operatore non autenticato utilizzando le credenziali di autenticazione di un addetto;

l'accesso effettuato aggirando il sistema di autenticazione;

l'accesso effettuato da un addetto autenticato in aree non previste dal sistema di autorizzazioni;

l'accesso tramite intercettazioni di informazioni in rete;

l'accesso non autorizzato a locali/aree ad accesso non riservato;

l'accesso a strumenti contenenti dati che sono stati sottratti.

- Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti e adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.
- Nel caso di azione di virus informatici verranno immediatamente bloccate tutte le operazioni su tutti i computer attraverso l'utilizzo di un programma antivirus aggiornato e verranno immediatamente verificati e bonificati tutti i computer.
- Nel caso di spamming verranno immediatamente bloccate tutte le operazioni su tutti i computer ed il Consulente Informatico disattiverà momentaneamente tutte le connessioni con Internet, verificherà i firewall su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer.
- Nel caso di azione dei programmi suscettibili di recare danno verranno immediatamente bloccate tutte le operazioni su tutti i computer ed il Consulente Informatico disattiverà i programmi dannosi e verranno immediatamente verificati e bonificati tutti i computer.

In relazione a quegli eventi dannosi che comportano un elevato livello di criticità per il dato personale stesso, l'Azienda ha previsto un tempo di ripristino pari a 5 giorni per i seguenti casi di violazioni illecite o accidentali di dati:

Perdita, Distruzione, Modifica, divulgazione non autorizzata, Accesso ai dati personali che siano trasmessi, conservati o trattati.

Al fine di ripristinare gli archivi e dati, si è provveduto a conservare in un luogo esterno alla sede, copie aggiornate settimanalmente dei dati.

FORMAZIONE DEL PERSONALE

Sono previsti incontri formativi per tutti gli addetti con la finalità di rendere loro edotti su:

- sulla segretezza della componente riservata della credenziale e sulla diligente custodia dei dispositivi in possesso ed uso esclusivo dell'addetto;
- sulla custodia e l'accessibilità degli strumenti informatici;
- sul controllo e sulla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- sulle procedure aziendali da applicare per la sicurezza e la protezione dei dati;
- sulle Policy aziendali in riferimento all'utilizzo della posta elettronica ed internet e sul sistema di videosorveglianza;
- sulle azioni relative alle procedure da attivare per risolvere o per contenere l'effetto negativo scaturito dall'eventuale evento dannoso;
- sulle definizioni ed i ruoli del Regolamento 679/2016 e sui diritti degli interessati.

AUTORITÀ DA CONTATTARE IN CASO DI EMERGENZA

Il Titolare del Trattamento a norma dell'art. 33 del Regolamento, qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (Considerando n.85), è tenuto entro massimo 72 ore (salvo giustificato motivo) dal momento in cui ne è venuto a conoscenza, la notificazione presso l'autorità competente, di cui all'art.55, della avvenuta violazione.

Nel caso di violazione che comporti un rischio elevato per i diritti e le libertà delle persone fisiche la comunicazione va fatta senza ingiustificato ritardo all'interessato, ai sensi dell'art.34.

VALUTAZIONE IMPATTO PRIVACY

Valutando le criticità emerse dalla valutazione dei rischi si può considerare il livello di rischio dell'Azienda come BASSO constatandosi che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati.

DEFINIZIONI PRINCIPALI NORMATIVA PRIVACY

Titolare del Trattamento: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

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

Somel Impianti Srl

Sede e Uffici
Via Francesco Rolla 6/8 r
Via Angelo Bagnara 10-12 r
e-mail: info@somelimpianti.it
web: www.somelimpianti.it
16152 Genova Cornigliano
Tel / Fax +39 010 6518197

C.C.I.A.A. Genova n° 263336
Tribunale di Genova n° 11637
Società n° 36716/54477
Codice Fiscale e Partita Iva 01185840103

Destinatario: persona fisica o giuridica, l'autorità pubblica; il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a 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.

Dato sensibile: dati personali idonei a rivelare 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, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.

Dato giudiziario: dati personali idonei a rivelare informazioni 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.

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia, sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

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

Dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Trattamento (dei Dati): qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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.

Prima emissione: in data 02/07/2018

Prima revisione: in data 26/07/2021

Seconda revisione: in data 29/04/2022 (x cambio ragione sociale)