REGOLAMENTO PRIVACY

POLICY IT

in attuazione del Regolamento UE 2016/679

Titolare:
Conceria Settebello S.p.A.
Via XXV Luglio, 32
56029 - Santa Croce sull'Arno (PI)

Data ultima revisione documento:

01.04.2019

Approvato da

Il Titolare del Trattamento dei Dati

(

INDICE

1. Stato di revisione del documento

In riferimento all'obbligo, di aggiornare ed implementare il sistema di protezione e sicurezza dei dati, previsto dal GDPR 679/2016, l'azienda si impegna a dare evidenza degli aggiornamenti intervenuti nel corso del tempo.

STATO DI REVISIONE	DESCRIZIONE
Revisione del **01.04.2019**	Prima emissione del documento

2. Definizioni (art. 4 GDPR679/2016)

Ai fini del presente Privacy Policy si intende per:

- **«Regolamento Privacy» «privacy policy»**: si intende il regolamento aziendale sulla privacy di **Conceria Settebello Spa**;
- **«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;
- **«dati riservati»**: atti giudiziari, informazioni commerciali, accordi di riservatezza, ecc.
- **«trattamento»**: 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;
- **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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 tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- **«titolare del trattamento»**: la 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;
- **«destinatario»**: la 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;
- **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **«violazione dei dati personali»**: la 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;
- **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati biometrici»**: i 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»**: i 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;
- **«stabilimento principale»**:

a. per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b. con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi della presente privacy policy; **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma della presente privacy policy;

- **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c. un reclamo è stato proposto a tale autorità di controllo; **«trattamento transfrontaliero»:**

a. trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b. trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;**«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione della presente privacy policy, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme alla presente privacy policy, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. Scopo e campo di applicazione

Il presente documento, ha l'obiettivo di attuare adeguate misure di sicurezza nella gestione del trattamento dei dati personali in all'interno dell'azienda.

Questo documento fornisce agli Autorizzati al trattamento dati (di seguito "Autorizzati") istruzioni e linee guida sui compiti loro spettanti in merito alla gestione ed allo sviluppo della sicurezza nel trattamento di dati personali.

Viene, altresì, regolamentato l'utilizzo di internet e posta elettronica per utenti di tali servizi nell'ambito della struttura aziendale.

L'inosservanza della Legge può comportare sanzioni di natura civile, amministrativa e penale per l'Autorizzato e per l'azienda per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni riportate.

Le presenti istruzioni si applicano:

- a tutti i lavoratori dipendenti e a tutti i collaboratori di **Conceria Settebello Spa** a prescindere dal rapporto contrattuale con la stessa intrattenuti (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, ecc…)
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale

4. Contesto dell'organizzazione

Dati generali

Denominazione	**Conceria Settebello Spa**
Stato giuridico	Società per Azioni
Sede legale	Via XXV Luglio, 32 – 56029 Santa Croce sull'Arno (PI)
Telefono	0571 366760
Sito internet	www.settebelloconceria.it
E-mail	info@settebelloconceria.it
Cod. Fiscale e P. IVA	00205010507
Attività svolta	Lavorazione pelli
Rappresentante Legale	Marco Brogi

5. Compiti e responsabilità

Le figure coinvolte in azienda del trattamento vengono di seguito riportate

Titolare	**Conceria Settebello Spa**
Autorizzati/Incaricati	Formalizzata nomina riportante compiti e responsabilità
Responsabili Esterni	Formalizzata nomina riportante compiti e responsabilità

Le figure dei suddetti Responsabili e Autorizzati sono state nominate con atti formali utilizzando idonea modulistica (**DOC.P03- DOC.P04 - DOC.P05 -DOC.P07**)

6. Titolare del Trattamento

Conceria Settebello Spa come titolare del trattamento (ai sensi dell'art. 28 d.lgs n.196/2003 e art. 4 co. 1, n.7 GDPR) provvede:

- ad assolvere agli obblighi di notificazione previsti dal GDPR;
- ad assolvere all'obbligo delle valutazioni di impatto privacy ai sensi dell'art. 35 GDPR (data protection impact assessment);
- a richiedere al Garante pareri in merito a trattamenti di dati personali che presentano rischi elevati per gli interessati;
- a nominare, con proprio atto, i Responsabili esterni del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 15 del GDPR;
- alla sicurezza dei trattamenti ai sensi dell'art. 32 del GDPR;
- a nominare il Data Protection Officer nei casi previsti dalla legge (art. 37 GDPR);
- disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.

7. La figura del responsabile esterno del trattamento ex art. 28 GDPR

Conceria Settebello Spa nella gestione dei trattamenti esternalizzati di dati personali, provvederà all'individuazione e nomina dei responsabili esterni del trattamento. (**DOC.P03- DOC.P04 - DOC.P05**)

Il Responsabile del trattamento esterno è il soggetto, designato per iscritto dal Titolare, che, ai sensi dell'art.28 del GDPR deve garantire per esperienza, capacità ed affidabilità, il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali limitatamente ai trattamenti oggetto del rapporto contrattuale.

Il Responsabile potrà nominare ulteriori sub-responsabili previa autorizzazione al titolare del trattamento (art. 28 del GDPR).

8. Autorizzati/Incaricati del trattamento

Ai sensi dell'art. 4, n. 10 del GDPR, sono Incaricati/Autorizzati del trattamento le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare, attenendosi alle istruzioni impartite. La designazione è fatta per iscritto. Tutti i lavoratori che in **Conceria Settebello Spa** trattano dati personali sono stati designati Autorizzati al trattamento (**DOC.P07**).

Gli incaricati hanno accesso ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti aziendali loro assegnati. Durante il trattamento in caso di allontanamento dal posto di lavoro, l'incaricato deve adottare le misure previste secondo le istruzioni ricevute dal Titolare contemplate nel presente regolamento.

9. Trattamenti dei dati personali

Nel Registro delle attività di trattamento (**DSP-01)** è riportata una ricognizione completa in forma schematica dei trattamenti effettuati da **Conceria Settebello Spa** raggruppati per categoria di dati e riportanti per ciascuna categoria, finalità, natura dei dati, autorizzati interni, responsabili esterni, base giuridica dei trattamenti, durata, strumenti utilizzati, categorie di rischio e misure di sicurezza.

Per mero scrupolo, si specifica – anche alla luce del dettame ex Regolamento UE 679/2018 – i dati più significativi sono i dati dei dipendenti – in qualità di persone fisiche – che vengono trattati esclusivamente per gli adempimenti di legge e contrattuali e possono contenere Dati Sensibili / Particolari categorie di dati, quali l'eventuale iscrizione al sindacato o sullo stato di salute e/o Dati Giudiziari.

10. Modalità di trattamento

All'interno della **Conceria Settebello Spa** il trattamento dei dati personali può avvenire con o senza strumenti elettronici. Gli Autorizzati, che per mansioni ricoprono ruoli di direzione, sono tenuti a vigilare sulla corretta gestione dei trattamenti.

11. Infrastrutture e risorse da proteggere

Conceria Settebello Spa si avvale di una serie di risorse attraverso le quali procede al trattamento dei dati personali.

Le risorse di cui sopra possono essere opportunamente suddividere e analizzate a seconda della tipologia:

- ❒ Siti Fisici. Trattasi dei luoghi in cui fisicamente avviene il trattamento dei dati. In questi locali, che possono essere uffici, magazzini o altro, sono ubicati i sistemi di elaborazione (PC, Server, etc.) e/o ogni altra attrezzatura ritenuta idonea al contenimento dei dati.
- ❒ Archivi dati. Trattasi di tutti gli archivi in cui sono contenuti dati personali trattati dall'azienda. Per archivi, se non meglio specificato s'intenda sia quelli elettronico-informatici sia quelli su supporto cartaceo.
- ❒ Risorse Informatiche
    - Hardware: Risorsa Hardware è qualsiasi apparecchiatura elettronica utilizzata per compiere operazioni di trattamento di dati personali. In particolare la rete del sistema informativo, utilizzato per la conservazione dei dati in formato elettronico, ed i PC (Personal Computer) con cui sono eseguiti i programmi idonei all'elaborazione del trattamento.
    - Software: Sono i programmi installati sui PC con cui sono eseguiti i programmi idonei all'elaborazione del trattamento.

11.1 Sede ed infrastrutture

Gli accessi alla sede sono presidiati da un sistema di allarme e durante l'orario lavorativo sono gestiti e controllati dal personale presente in azienda. Non sono comunque previsti accessi al pubblico.

Gli uffici sono dotati di chiusura a chiave.

E' presente un sistema antincendio (estintori con regolare manutenzione e formazione ad hoc dipendenti).

11.2 Risorse informatiche

In azienda sono presenti:

- n. 20 PC operativi distribuiti tra la sede legale ed i reparti produttivi di Via XXV Luglio e Via Puglia – Santa Croce sull'Arno (PI)

- Gestionale Contabilità AS400

- n. 1 Server sito in locale chiuso a chiave

L'accesso alle risorse è possibile soltanto attraverso l'utilizzo di credenziali di accesso (username e PW) personali, in osservanza a quanto disposto dalle normativa in materia.

11.3 Archivi cartacei

I supporti cartacei sono raccolti presso le singole postazioni, nonché in armadi e cassetti dove si provvede ad archiviare quotidianamente i supporti di comune e continuo utilizzo.

Quanto ai dati sensibili presenti su supporto cartaceo questi sono archiviati in armadi dotati di serratura le cui chiavi sono affidate ai soli incaricati autorizzati a quel particolare trattamento come da specifico atto di autorizzazione/nomina/incarico.

12. Obbligo di segnalazione- Data Breach (art. 33 GDPR)

Ogni Autorizzato deve segnalare alla Direzione privacy di **Conceria Settebello Spa** ogni sospetta anomalia nel trattamento di dati personali o ogni sospetta violazione della Legge ed è altresì obbligato a riferire immediatamente alla stessa l'eventuale esercizio dei diritti da parte degli Interessati (le persone i cui dati vengono trattati) o ogni richiesta avanzata da questi ultimi

affinchè il Titolare del trattamento stesso possa prendere gli opportuni provvedimenti ai sensi della Legge.

In caso di sospetta o riscontrata violazione dei dati personali, gli Autorizzati dovranno immediatamente informare la Direzione per la notifica all'Autorità di Controllo competente (che deve essere effettuata senza ingiustificato ritardo e entro 72 ore dal momento in cui se ne è venuti a conoscenza).

Gli Autorizzati, devono, altresì rivolgersi al Titolare per ogni eventuale dubbio applicativo o interpretativo in materia di trattamento dei dati personali.

13. Linee guida per il trattamento dei dati personali

Di seguito vengono descritte le norme a cui gli Autorizzati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Innanzitutto occorre rilevare che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali del trattamento, l'Autorizzato deve osservare le seguenti prescrizioni:

- ❑ 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 come confidenziali e, di norma, soggetti a segreto;
- ❑ 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, 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 (es. blocco PC) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- ❑ non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal Titolare del trattamento;
- ❑ devono essere eseguite esclusivamente operazioni di trattamento necessarie per il raggiungimento dei fini per i quali sono stati raccolti;
- ❑ deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra indicato impone, pertanto, 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.

Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

13.1 *Accesso ai dati dalla postazione di lavoro*

Accesso fisico ai locali:

1) I locali, dove sono custoditi i dati personali (in particolare quelli sensibili), devono essere soggetti a controllo e verifica, al fine di evitare che durante l'orario di lavoro possono essere conosciuti o accessibili da parte di soggetti non autorizzati.

2) Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non è legittimato, soprattutto se esterno all'organizzazione di appartenenza.

3) Durante l'orario lavorativo i terzi (ospiti, clienti, fornitori consulenti ecc.) che accedono ai locali dell'azienda devono essere identificati.

4) Al termine della giornata di lavoro e in caso di allontanamento dalla propria postazione è necessario assicurarsi della chiusura della porta di accesso, nonchè di aver riposto i documenti nei cassetti della propria scrivania o nei rispettivi archivi. Tali operazioni dovranno essere eseguite ogni volta occorre allontanarsi dalla propria postazione di lavoro.

La postazione di lavoro deve essere, inoltre:

- ❑ utilizzata solo per scopi legati alla propria attività lavorativa;
- ❑ utilizzata in modo esclusivo da un solo utente;
- ❑ protetta, evitando che terzi possano accedere ai dati che si stanno trattando.

Occorre, inoltre, precisare che è **dovere dell'Autorizzato**:

- ❑ non utilizzare all'interno dell'azienda risorse informatiche personali private (PC, periferiche, token, chiavi USB ecc..);
- ❑ non installare alcun software;

- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc..);
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+Alt+CAN) ed assicurarsi dell'attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo massimo 5 minuti di inattività;
- non lasciare eventuali computer portatili incustoditi sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante le riunioni lontane dalla propria postazione);
- non trasmettere in alcun modo informazioni riservate e dati personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e/o se esso non è legittimato a riceverle.
- non consentire l'accesso a personale esterno non Autorizzato; in caso di interventi di manutenzione autorizzati dal Titolare (es. installazione di nuovo software/hardware nel computer), occorre assicurarsi dell'identità della persona e delle autorizzazioni per operare sul PC.

13.2 *Gestione della Password*

Nell'adeguare i sistemi informatici dell'azienda alle disposizioni legislative in tema di sicurezza è stato introdotto l'uso di diverse chiavi di accesso (user ID e Password) alle risorse informatiche contenenti dati personali.

È necessario mantenere il massimo riserbo in relazione alle proprie chiavi di accesso ed è espressamente vietato comunicarle ad altri Autorizzati (in tal caso, terze persone accederebbero alle risorse di rete sotto l'identità digitale dell'Autorizzato e qualsiasi operazione abusiva venisse effettuata sarebbe attribuita alla responsabilità dello stesso identificato dalla chiave di accesso).

Per una corretta gestione della password, si deve aver cura di:

- cambiarla almeno ogni 6 mesi o immediatamente nei casi in cui sia compromessa o si abbia notizia o timore che la propria password abbia perso la propria riservatezza;
- comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico lo consenta, con un numero di caratteri pari al massimo consentito;
- usare sia lettere che numeri e almeno uno con carattere maiuscolo;
- non basare la scelta su informazioni facilmente deducibile, (es. proprio nome, nome di familiari, date di nascita, date anniversari, codici fiscali ecc..);

- mantenerla riservata e non divulgarla a terzi;
- non permettere ad altri utenti (es. colleghi, collaboratori ecc..) di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it ..) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;
- quando si immette la password nei form di richiesta, evitare che altri possano vedere i tasti che si battono sulla tastiera.
- NON utilizzare sempre la stessa password per tutti i sistemi.

13.3 *Prevenzione da infezioni di virus informatici*

I PC in dotazione, pur protetti contro gli attacchi dei virsus informartici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.

Come prevenire i virus:

Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare periodicamente, che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
- chiudere correttamente i programmi in uso;
- non aprire file sospetti e di dubbia provenienza e utilizzare solo documenti, immagini, file in generale, provenienti da fonti conosciute ed affidabili;
- non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate dal Titolare;
- non utilizzare unità di memoria non autorizzate specificatamente da **Conceria Settebello Spa** ed altri supporti elettronici di dubbia provenienza;
- verificare con l'ausilio del programma antivirus in dotazione ogni supporto digitale autorizzato e contenente dati (chiavetta USB o CD-Rom), prima dell'esecuzione dei file in esso contenenti e proteggere i dispositivi di memoria da scrittura (quando possibile);
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale nel PC;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
- non modificare le configurazioni impostate sul proprio PC;

- ❑ spegnere il PC al termine della giornata di lavoro.
- ❑ Utilizzare soltanto programmi autorizzati dal Titolare

In caso di malfunzionamento del PC che può far sospettare la presenza di un virus, è buona regola:

a) Sospendere ogni operazione sul PC evitando di lavorare con il sistema infetto;

b) Contattare immediatamente il Titolare del trattamento

13.4 *Salvataggio dei dati*

1) Tutti i dati al termine della giornata lavorativa vengono salvati sul server.

2) A tal proposito, qualora vi sia la necessità, si può richiedere al Titolare del trattamento la creazione sul server di una cartella intestata, in alternativa, ad una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Autorizzato stesso.

3) I file contenenti dati particolari o sensibili devono essere salvati e protetti con password di accesso al documento.

13.5 *Protezione dei PC portatili e dispositivi mobili (smartphone, tablet)*

I dispositivi mobili presentano maggiori vulnerabilità rispetto ad una postazione fissa di lavoro.

Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono riportate ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- ❑ Conservare il dispositivo in un luogo sicuro alla fine della giornata lavorativa;
- ❑ Non lasciare mai incustodito il dispositivo in caso di utilizzo in ambito esterno all'azienda;
- ❑ Avvertire tempestivamente il titolare, che darà le dovute indicazioni, in caso di furto/smarrimento;
- ❑ Essere sempre ben consapevole delle informazioni archiviate sui dispositivi mobili, maggiormente soggetti a furto e smarrimento rispetto alla postazione fissa;
- ❑ Operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le Password potrebbero essere intercettati da osservatori indiscreti.
- ❑ Effettuare frequenti backup dei dati.

13.6 *Uso di Internet e della Posta elettronica*

Gli strumenti di comunicazione telematica (Internet e Posta Elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative.

Tutte le informazioni archiviate negli elaboratori e nei sistemi di comunicazione dell'azienda (inclusi documenti, altri files, messaggi di posta elettronica e le registrazioni dei messaggi di posta vocale) sono di proprietà di **Conceria Settebello Spa**.

Si precisa che indirizzi di posta elettronica assegnati agli utenti sono di proprietà **Conceria Settebello Spa** che si riserva di utilizzarli anche dopo la cessazione del rapporto di lavoro per un periodo massimo di 6 mesi dopodichè verranno definitivamente disattivati.

Per scopi personali si devono utilizzare i propri dispositivi personali ed account privati di posta elettronica (a pagamento o gratuiti).

Tutta la corrispondenza elettronica attinente a questioni di lavoro deve essere mantenuta attraverso l'account di posta elettronica ufficiale messo a disposizione dalla Società. È vietato inviare o chiedere di farsi inviare su account privati messaggi o documenti elettronici attinenti al lavoro.

Sono vietati comportamenti che possono arrecare danno all'azienda o comportare rischi per i dati personali.

Pertanto, si dovranno osservare le prescrizioni di seguito riportate:

- ❑ è consentita la navigazione Internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate,
- ❑ non è consentito scaricare software gratuiti (freeware o shareware) da siti Internet;
- ❑ non è consentita la registrazione a siti Internet o partecipare a forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- ❑ l'accesso alla rete Internet non può essere utilizzato per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività della Società.
- ❑ non è consentito l'utilizzo di funzioni instant messaging a meno che non siano autorizzate da **Conceria Settebello Spa** o, comunque, in linea con quanto previsto nel presente documento;
- ❑ è vietato aprire e-mail e file allegati di origine sconosciuta o che prestino degli aspetti anomali (es. un soggetto non chiaro);
- ❑ non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- ❑ è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;

- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso di dati che ci si appresta ad inviare;
- occorre sempre essere consapevoli che posta elettronica e navigazione Internet sono veicoli per l'introduzione sul proprio strumento informatico (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati;
- è vietato installare autonomamente programmi, sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dall'azienda;
- è vietato modificare le caratteristiche impostate sulle dotazioni o installare dispositivi di memorizzazione, comunicazione o altro, collegare alla rete aziendale qualsiasi apparecchiatura (es. switch, hub, apparati di memorizzazione di rete), effettuare collegamenti verso l'esterno di qualsiasi tipo (es. tramite modem o connect card) utilizzando un PC che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale e la rete esterna);
- al fine ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere *"tenuta in ordine"*, cancellando periodicamente documenti inutili o allegati ingombranti;
- va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (es. chiavi USB, dischi esterni ecc..), avvertendo immediatamente il titolare nel caso in cui siano rilevati virus;
- i sistemi di comunicazione della Società non possono essere utilizzati per creare, custodire o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, denigrazioni, epiteti ovvero qualsiasi altra cosa che possa essere considerata una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose. Allo stesso modo, i sistemi di comunicazione aziendale non possono essere utilizzati per sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività aziendale.
- anche nel caso di eventuale utilizzo della posta elettronica di **Conceria Settebello Spa** tramite connessioni remote (VPN, WEBMAIL, ecc.) valgono tutte le regole finora enunciate. In aggiunta è fatto divieto di copiare informazioni (ad esempio allegati) sui sistemi di elaborazione personali utilizzati per la connessione remota stessa, con eccezione degli

eventuali dispositivi mobili dati in dotazione dall'Azienda con atto scritto.

In caso di assenza programmata (ferie, attività di lavoro fuori sede) si deve attivare l'apposita funzionalità di sistema, ovvero il *"fuori sede"*, che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (elettroniche o telefoniche) di un altro Autorizzato o altre modalità utili di contatto della struttura.

In caso di mancata attivazione di tale risposta automatica (per dimenticanza o per assenza non programmata), è facoltà di **Conceria Settebello Spa** attivare tale meccanismo di risposta automatica anche senza la presenza dell'Autorizzato.

L'azienda in caso di improvvisa o prolungata assenza dell'Autorizzato o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva di accedere alla casella di posta elettronica dell'Autorizzato assente.

13.7 *Particolari attenzioni nell'invio di documenti*

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando il dato deve essere inviato via fax, posta elettronica ecc..,, e soprattutto, laddove vengano inviati documenti contenenti dati personali occorre:

- prestare la massima attenzione affinché il numero telefonico/fax o l'indirizzo mail immessi siano corretti;
- Per il fax verificare che non ci siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario della quantità di pagine inviate;
- nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

13.8 *Documenti e Archivi cartacei*

Tutto il materiale cartaceo contenete dati personali - ed in modo particolare quelli sensibili considerata la natura dell'attività svolta da **Conceria Settebello Spa** - non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in luogo sicuro.

I documenti stampati o fotocopiati devono essere ritirati quanto prima ed è necessario verificare sempre che non ci siano documenti in attesa di essere stampati.

Allorché una stampa non sia più utile sarà necessario procedere alla distruzione della stessa. Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrice o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento con qualsiasi mezzo che ne renda impossibile la ricostituzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi

Inoltre, occorre usare la stessa attenzione nello svolgimento delle normali operazioni quotidiane di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati particolarmente sensibili (stato di salute, dati giudiziari), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato dalla proprietà.

Le riproduzioni di documenti contenenti dati sensibili e/o informazioni relative al trattamento di dati personali devono essere conservati e custoditi con le medesime modalità previste per i documenti originali.

14. Monitoraggio e controlli da parte della proprietà aziendale

In questa sede si riporta all'attenzione degli Autorizzati la possibilità di **Conceria Settebello Spa** di effettuare controlli sulle proprie risorse informatiche al fine di preservare la sicurezza delle stesse e dei dati ivi contenuti, ivi inclusa in particolare la protezione dei dati personali.

A tal fine si sottolinea che la strumentazione tecnologica/informatica e quanto con essa è creato è di proprietà dell'azienda in quanto mezzo di lavoro.

È, pertanto, fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esse effettuate per fini ed interessi non strettamente coincidenti con quelli dell'azienda stessa.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti, degli interessati e del presente documento.

In caso di anomalie, **Conceria Settebello Spa,** per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso al Titolare, affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite o che comportino rischi per l'azienda nonché per i diritti e le libertà fondamentali degli interessati.

In nessun caso verranno realizzate verifiche prolungate, costanti ed indiscriminate, fatte salve le verifiche atte a tutelare la adeguata protezione dei dati personali.

15. Informativa e consenso

Conceria Settebello Spa ha provveduto ad informare nei modi e nelle forme previste dalla legge tutti gli interessati dei trattamenti in essere. In occasione di nuovi trattamenti di dati personali la relativa modulistica viene messa a disposizione da parte del Titolare stesso.

16. Dipendenti e assimilati

Al personale dipendente, ai soggetti con i quali vengono instaurati rapporti di collaborazione (*stagista, interinale ecc.*), viene fornita l'informativa privacy di rito in sede di instaurazione dei relativi rapporti.

17. Il trattamento dei dati sensibili e giudiziari

Tutto il personale che presta servizio, a qualsiasi titolo, presso l'azienda è tenuto a trattare gli eventuali dati sensibili e giudiziari indispensabili per l'espletamento delle mansioni di competenza con modalità tali da garantire il rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato.

18. Comunicazione e diffusione

Particolare attenzione deve essere prestata da tutti gli incaricati qualora le operazioni di trattamento, note come comunicazione e diffusione, coinvolgano i dati sensibili e giudiziari. La comunicazione e diffusione dei dati è possibile a condizione che le stesse trovino copertura normativa in disposizioni legislative, fermo restando che i dati idonei a rivelare lo stato di salute non possono essere mai diffusi.

Qualsiasi comunicazione di dati sensibili e/o giudiziari deve ottenere l'approvazione preventiva dell'azienda.

19. Registro dei trattamenti

L'azienda ha redatto e tiene aggiornato un registro dell'attività di trattamento sulla base delle analisi dei rischi che incombono sui dati trattati dalle varie aree aziendali, delle misure in essere e da adottare per la messa in sicurezza dei dati medesimi.

20. Richieste di accesso agli atti

Qualsiasi richiesta di informazioni e/o accesso agli atti proveniente da qualsiasi interessato (lavoratori/utenti/ terzi) deve essere inoltrata tempestivamente al Direzione di **Conceria Settebello Spa**.

21. Piano di Emergenza e Ripristino (Contingency Planner e Disaster Recovery)

Il piano di emergenza deve consentire all'aziende di avere rapidamente a disposizione i dati informatici necessari, a seguito di un sinistro, doloso o accidentale. Tale piano viene messo in atto allorché si verifichi una situazione di emergenza che renda indisponibile uno o più dati o un suo trattamento.

Un corretto salvataggio periodico dei dati (back-up) su vari ed adeguati supporti concorre a mantenere l'integrità degli stessi, e soprattutto a mantenerne la disponibilità, nell'ottica di un'iniziativa di contingency planning e disaster recovery.

Il piano di emergenza deve permettere l'immediato ripristino dell'accesso ai dati elettronici nel minor tempo possibile e comunque non oltre 2 giorni successivi al verificarsi della indisponibilità degli stessi. Alla luce delle disposizioni di legge è evidente che l'obiettivo è il ripristino prioritario dei dati personali, attività di trattamento primaria che deve essere ripristinata prima di tutte le altre attività che possono essere riprese in un tempo superiore, che dovrebbe comunque contenersi al massimo in sette giorni.

I sistemi sono generalmente ospitati su server ad alta disponibilità che offrono una buona resilienza a situazioni di normali guasti tecnici e con dischi ridondati permettono di ripristinare la disponibilità dei dati in caso di guasto.

A tal fine vengono effettuate le seguenti operazioni:

1. Esecuzione giornaliera del back up attraverso procedure automatiche;
2. Report dei back up effettuati;

Ad oggi i backup, sono correttamente gestiti e la presenza di gruppi di continuità evita brusche interruzioni di corrente che potrebbero danneggiare gli elaboratori e rendere inutilizzabile il disco fisso.

22. Monitoraggio, controllo e verifica

La società, in quanto titolare dei dati trattati, provvede al monitoraggio ed al controllo periodico dell'efficacia delle misure di sicurezza poste in essere.

Durante queste operazioni di verifica, da effettuarsi al più ogni sei mesi, sarà data particolare importanza a:

- verifica rispetto delle disposizioni di cui al Manuale Privacy da parte degli incaricati
- verifica adeguato aggiornamento delle nomine degli incaricati interni
- verifica adeguato aggiornamento delle nomine dei responsabili esterni
- verifica della correttezza ed efficacia delle istruzioni, modulistica e procedure adottate soprattutto in presenza di variazioni organizzative e/o degli assets aziendali;
- verifica efficacia dei sistemi antintrusione
- verifica efficacia dei sistemi di videosorveglianza
- verifica aggiornamento dei dispositivi antivirus;
- verifica del corretto funzionamento del firewall;
- verifica aggiornamento e sicurezza dei programmi software che trattano i dati personali;
- verifica integrità dei dati e delle loro copie di backup
- verifica efficace funzionamento dei gruppi di continuità;
- verifica modalità di conservazione e utilizzo dei documenti cartacei
- accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati;
- accertamento del livello di formazione degli incaricati: prevedere sessioni di aggiornamento anche in relazione all'evoluzione organizzativa, tecnica e tecnologica avvenuta in azienda.
- verifica del rispetto delle istruzioni e procedure adottate, tra cui: utilizzo modulistica approvata per informative, nomine/incarichi, Corretto utilizzo delle password e dei profili d'accesso degli incaricati, disattivazione dei codici di accesso non utilizzati per più di sei mesi ecc.

23. Formazione

In occasione della realizzazione del Sistema per la protezione dei dati (come descritto nel presente documento) è stata effettuata la formazione ai referenti interni dell'azienda sui principi generali della normativa in materia di tutela della riservatezza dei dati personali.

Il Titolare del trattamento già all'atto di nomina degli Autorizzati al trattamento ha provveduto, provvede e provvederà a renderli edotti sui rischi individuati e sui modi per prevenire i danni, sulle misure di sicurezza, impartendo le dovute istruzione. Il Titolare del trattamento dei dati si impegna altresì a formare ed informare gli eventuali incaricati al trattamento che utilizzano gli elaboratori al fine di renderli edotti dei rischi individuati e dei modi per prevenire i danni.

Il personale autorizzato al trattamento dei dati personali verrà messo a conoscenza dei seguenti argomenti:

- spiegazione delle disposizioni di legge vigenti e applicabili in materia di protezione dei dati personali (principi di accountability, Privacy by Design e By Default, responsabilità, sanzioni);
- disposizioni legislative in tema di tutela dei dati e criminalità informatica;
- analisi e spiegazione dei ruoli tra cui: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato;
- cenni sul ruolo del Garante;
- principi di diligenza secondo il codice civile: i profili di responsabilità civile e penale; l'inversione dell'onere della prova (Art. 2050 C.C.);
- misure di sicurezza adeguate con particolare riferimento a: criteri logici, fisici, tecnici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare password antivirus e misure antihacker), contenitori di sicurezza, sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di backup, etc..

Coerentemente con l'evoluzione degli strumenti tecnici e organizzativi adottati dall'azienda e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi.

Periodicamente la Direzione aziendale garantirà lo svolgimento delle adeguate attività formative ed informative sull'importanza di adottare le norme per la sicurezza dei dati nonché le misure di controllo definite in relazione ai rischi individuati.

24. Sanzioni

L'Autorizzato, al fine di non esporre sé stesso e l'azienda a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla Legge, alle normative di volta in volta vigente ed applicabili ed alla regolamentazione aziendale.

L'Autorizzato, consapevole del corretto utilizzo dei servizi internet e della posta elettronica; è pertanto, responsabile per i danni eventualmente cagionati al patrimonio e alla reputazione dell'azienda.

Tutti gli Autorizzati sono, pertanto, tenuti ad osservare e a far osservare le disposizioni contenute nel presente documento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre l'adozione di provvedimenti di natura disciplinare e anche azioni civili e penali stabilite dalle leggi vigenti;
- per i collaboratori esterni oltre che la risoluzione del contratto, le azioni civili e penali stabilite dalle leggi vigenti.

25. Confidenzialità

Tutte le informazioni oggetto del presente Regolamento sono confidenziali e costituiscono patrimonio aziendale di **Conceria Settebello Spa** e sono tutelate dalle norme sulla riservatezza previste dall'ordinamento giuridico.

* * *

Principali riferimenti normativi, provvedimenti e atti interni

- Regolamento UE 2016/679 del Parlamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- Decreto Legislativo n. 196/2003 (Codice in materia di Protezione dei Dati Personali);
- Provvedimento Generale del Garante del 01/03/2007: "Linee guida sull'uso di internet e posta elettronica";

Conceria Settebello Spa