AUTORIZZAZIONE E ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI
RSPP
d.lgs 196/03 e GDPR 679/16

Gent.mo/a Sig./ra

ING. BIANCO ALBERTO

c/o **CHERASCO SRL**

VIA CADUTI SUL DON 38 12020 VILLAR SAN COSTANZO (CN)

Il sottoscritto **CHERASCO PIERGIUSEPPE**, legale rappresentante di **CHERASCO SRL** , con sede in **VIA CADUTI SUL DON 38 – 12020 VILLAR SAN COSTANZO (CN)**, in qualità di **Titolare del Trattamento dei Dati Personali**,

PREMESSO CHE:

- sia il d.lgs. 30 giugno 2003 n° 196, “Codice in materia di protezione dei dati personali”, che il GDPR 679/16 “Regolamento generale sulla protezione dei dati personali”, definiscono "dato personale", qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- entrambe le norme summenzionate intendono per "trattamento" dei dati personali, "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca di dati";
- sia il d.lgs. 30 giugno 2003 n° 196, “Codice in materia di protezione dei dati personali”, che il GDPR 679/16 “Regolamento generale sulla protezione dei dati personali”, fissano le modalità da adottare per detto trattamento ed individuano i soggetti che, in relazione all’attività svolta, sono tenuti agli adempimenti previsti dalla stessa legge;
- l'art. 30 del d.lgs. 196/03 prevede che il Titolare o il Responsabile del trattamento possa procedere alla nomina di uno o più incaricati del trattamento, i quali devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare o del Responsabile;
- l’art. 29 del GDPR 679/16 prescrive che chiunque agisca sotto l’autorità di un Responsabile o del Titolare del trattamento possa accedere ai dati personali solo se adeguatamente istruito;
- è interesse di **CHERASCO SRL** che il trattamento dei dati contenuti nelle proprie banche dati debba avvenire sotto il suo stretto controllo ed in conformità con le istruzioni tempo per tempo impartite;

TUTTO CIO' PREMESSO

considerato che il suo incarico di **RSPP** comporta, nell’esecuzione dell’attività lavorativa e per la durata dell’attività stessa, l’accesso ai dati personali;

considerato che lei svolgerà la sua mansione sotto l’autorità del Titolare del trattamento, identificato nella persona del legale rappresentante pro tempore della ditta;

con la presente lei è autorizzato ad effettuare sui dati personali, ivi compresi i dati sensibili idonei a rivelare lo stato di salute, contenuti nei giudizi di idoneità e nella gestione degli infortuni, le seguenti operazioni di trattamento:

- **Comunicazione**
- **Conservazione**
- **Consultazione**
- **Estrazione**
- **Organizzazione**
- **Raccolta**

Ogni trattamento dovrà essere effettuato in modo lecito, esplicito, legittimo e non eccedente le finalità della raccolta. I dati sopra elencati potranno essere trattati per le seguenti finalità:

- consegna al Titolare la copia della cartella sanitaria da consegnare ai lavoratori dimissionari;

- comunicazione dei giudizi di idoneità al Titolare e ai lavoratori;
- gestione operativa delle prescrizioni riportate dal medico competente (inidoneità, inidoneità parziale, limitazioni, uso di DPI o di altri ausili) nei giudizi di idoneità;
- archiviazione e conservazione dei giudizi di idoneità alla mansione;
- predisposizione e presentazione di rendiconti e rilevazioni di tipo statistico sui giudizi di idoneità alla mansione.

L'ambito del trattamento a lei consentito si applica sia ai dati contenuti in archivi e documenti cartacei che ai dati registrati e organizzati in archivi elettronici (basi di dati, liste, rubriche, ecc.) o inseriti in documenti e comunicazioni (email, form online, ecc.).

A tale fine vengono fornite le istruzioni necessarie per poter effettuare il trattamento.

Dette istruzioni sono disposizioni tassative, sono impartite dal Titolare del trattamento e la loro puntuale osservanza e applicazione viene controllata dal Titolare stesso o dal Responsabile del trattamento.

Istruzioni generali sul trattamento dei dati

Al fine di assicurarci che il trattamento venga effettuato nel pieno rispetto delle norme vigenti, rammentiamo il disposto dall'art. 11 d.lgs. 196/2003 e art. 5 GDPR 679/16, cioè che i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservati in una forma che consenta l'identificazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati.

Inoltre, facciamo osservare che si richiede particolare attenzione in merito ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

- rispetto delle procedure, anche informali, previste per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- osservanza delle prescrizioni, anche verbali, impartite in materia di reperimento dei documenti contenenti dati personali e di modalità di loro custodia e archiviazione;
- attuazione precisa delle regole di elaborazione e custodia delle password, necessarie per accedere agli elaboratori ed ai dati in essi contenuti;
- scrupoloso rispetto della prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- rispetto rigoroso delle procedure, anche informali, e delle modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché delle procedure definite per il salvataggio dei dati;
- osservanza delle istruzioni impartite, anche verbalmente, in tema di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali.

Modalità di generazione, sostituzione e conservazione delle credenziali di autenticazione

A ciascun utilizzatore del sistema informativo è assegnato un identificatore d'accesso (denominato login-id) per poter accedere alle risorse di rete (documenti, applicazioni, email, ecc.) o, tramite connessione internet, ad altri sistemi esterni (home banking, Inail, Inps, Intrastat, Entratel, ecc).

Al login-id è abbinata una chiave di accesso (password) necessaria per poter utilizzare il login-id stesso: la coppia di informazioni composto da login-id e password garantisce l'identità e l'univocità dell'utilizzatore. Per tale motivo, e sotto la responsabilità dell'utente, la password deve essere mantenuta segreta e non comunicata, o ancor peggio condivisa con altri. Allo stesso modo la password non deve mai essere trascritta su alcun supporto cartaceo.

Qualora si ritenga che la segretezza della propria password sia stata violata, si deve provvedere immediatamente o cambiarla, richiedendo ausilio al competente Ufficio IT o all'amministratore di sistema.

Le credenziali di accesso alla “postazione di lavoro” sono fornite dal competente Ufficio IT o dall’amministratore di sistema all’incaricato al momento dell’assunzione, del rientro in servizio o dell’inizio di una nuova mansione.

Alla prima assegnazione, l’utente – non appena effettuata l’autenticazione - dovrà provvedere a sostituire la password con una che risponda ai requisiti minimi di sicurezza:

- lunghezza minima 8 caratteri,
- assenza di riferimenti espliciti all’incaricato stesso (es.: cognome, nome, codice di accesso, USERID, ecc.),
- scadenza, con sostituzione obbligatoria, almeno trimestrale.

Circa venti giorni prima della scadenza il sistema, mediante avviso, ricorda e sollecita il cambiamento della propria password.

Inoltre, è fatto obbligo di attenersi a quanto segue:

- ogni utente è invitato a individuare un proprio fiduciario, autorizzato ad accedere alla casella di posta elettronica in caso di assenza improvvisa o prolungata dell’utente stesso; i responsabili delle unità organizzative comunicano al Responsabile del trattamento, o all’amministratore di sistema nome e cognome del fiduciario prescelto;
- nel caso in cui improrogabili esigenze di lavoro richiedano l’accesso a cartelle personali o a messaggi di posta elettronica conservati nella casella dell’utente assente o impossibilitato all’accesso, la Direzione potrà chiedere al fiduciario di accedere alle cartelle o alla casella di posta in questione e di verificare il contenuto dei files o messaggi rilevanti; il delegato riferirà i "dati rilevati" necessari per lo svolgimento dell'attività lavorativa al superiore gerarchico dell’utente assente.
- la Direzione redigerà apposito verbale, copia del quale sarà consegnato all’utente interessato al suo rientro al lavoro;
- nel caso in cui l’utente non abbia provveduto ad indicare il proprio fiduciario, sempre che improrogabili esigenze di lavoro richiedano l’accesso alle cartelle personali o ai messaggi di posta elettronica conservati nella casella dell’utente, la Direzione potrà richiedere all’amministratore di sistema di effettuare l’accesso - mediante l’utilizzo delle password di configurazione - e di svolgere il compito normalmente affidato al fiduciario. Anche in questo caso, la Direzione redigerà apposito verbale, copia del quale sarà consegnato all’utente interessato al suo rientro al lavoro.

Modalità operative da seguire per il trattamento dei dati

Al fine di effettuare correttamente i trattamenti oggetto dell’incarico ricevuto, la invitiamo ad attenersi alle indicazioni che seguono:

- richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa e pertinenti con la propria mansione;
- custodire i dati oggetto di trattamento in luoghi non accessibili a soggetti non autorizzati;
- non lasciare incustodito il posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
- non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedere all’archiviazione definitiva dei supporti cartacei e dei supporti magnetici o ottici nei luoghi a ciò predisposti, una volta che siano terminate le ragioni della consultazione;
- custodire con attenzione e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici;
- accertarsi che gli interessati abbiano ricevuto l’informativa in merito ai trattamenti effettuati e, ove necessario, abbiano espresso il consenso per i trattamenti che lo richiedono;
- accertarsi dell’identità dei terzi e della loro autorizzazione al ritiro di documentazione in uscita;
- astenersi dal fornire telefonicamente, o a mezzo fax, dati personali senza specifica autorizzazione e senza precisa identificazione del richiedente.

Limitazioni o esclusione di attività nell’uso delle risorse informatiche

Per effettuare i trattamenti previsti dalla mansione, le viene concesso l’utilizzo di alcune risorse informatiche (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa), le quali costituiscono strumenti di esecuzione delle normali prestazioni di lavoro.

Il loro uso deve sempre essere improntato al principio di comune buon senso e di civiltà. Pertanto, al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, garantire un elevato livello di sicurezza dei trattamenti e assicurare la protezione della riservatezza di dipendenti e collaboratori, è vietato:

- rispetto all'utilizzo del computer:
  - accedere e utilizzare le risorse ed i servizi per motivi non lavorativi o non di servizio;
  - usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o commettere attività illecite o discriminanti;
  - modificare le configurazioni impostate;
  - installare e utilizzare prodotti software che non siano stati autorizzati;
  - installare, utilizzare software che consentano di intercettare il traffico o violare le password;
  - usare le risorse o i servizi per scopi commerciali, promozionali, pubblicitari;
  - utilizzare eccessivo spazio disco o assorbire capacità di banda nei sistemi di telecomunicazione, attraverso la generazione o l'invio di mail non strettamente correlate all'attività lavorativa, o in generale, attraverso il trasferimento di file o messaggi di dimensioni eccessive;
  - inviare o depositare sui computer materiale di natura illegale o discriminante;
  - mascherare la propria identità all'interno dei sistemi informatici;
  - utilizzare le credenziali di autenticazione di altri utenti, per qualsivoglia ragione;
  - tentare di violare password, sistemi di protezione, restrizioni imposte dal sistema;
  - riprodurre o distribuire materiale in formato digitale senza autorizzazione;
  - copiare o modificare files, redatti da altri utenti, senza autorizzazione;
  - alterare i dati, introdurre o diffondere virus, trojan, backdoor, dataminer o altri codici malefici;
  - interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
  - intercettare o alterare qualunque tipo di dato o di comunicazione digitale.

- rispetto all'utilizzo di internet
  - navigare su siti non correlati con la prestazione lavorativa;
  - effettuare download di programmi e files estranei al lavoro;
  - partecipare a forum, accedere e utilizzare chat line, partecipare ad aste on-line;
  - scaricare, copiare, conservare, diffondere file a contenuto offensivo, discriminatorio, pedofilo, o di altro contenuto illecito penalmente o civilmente;
  - accedere a siti di gioco, pornografici o con finalità ludiche;
  - attivare strumenti di videochiamata (es.: skype).

- rispetto all'utilizzo della posta elettronica
  - utilizzare la posta elettronica per ragioni non attinenti ai compiti affidati;
  - inviare, stampare, conservare messaggi offensivi o discriminatori; .
  - comunicare indirizzi di posta riconducibili al Titolare per partecipare a dibattiti, forum o mailing list di contenuto non pertinente con lo svolgimento delle mansioni affidate;
  - creare cartelle segrete o nascoste per la conservazione dei messaggi.

Limiti di effettuazione dei trattamenti consentiti

In ogni caso, lei dovrà rispettare in modo rigoroso i seguenti limiti:

- senza preventiva autorizzazione del Titolare del trattamento, o del Responsabile del trattamento, non le sarà possibile creare nuovi archivi o nuove banche dati;
- non dovrà comunicare a terzi gli esiti delle interrogazioni delle banche dati.
- dovrà conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, sussiste l'obbligo di restituire gli stessi al termine delle operazioni affidate;
- è concesso di utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili; altrimenti occorre etichettarli e riporli negli appositi contenitori;
- le copie di dati personali su supporti amovibili sono permesse solo se costituiscono parte indispensabile del trattamento;
- le copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento. In ogni caso i supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento;

- ogni comunicazione di dati verso l'esterno, che non costituisca oggetto di specifico compito già affidato, deve essere autorizzata preventivamente dal Titolare del Trattamento o dal Responsabile del trattamento;
- la diffusione dei dati è tassativamente proibita, salva preventiva autorizzazione del Titolare del trattamento;
- i divieti di comunicazione e di diffusione summenzionati, permangono anche dopo la cessazione dell'incarico ricevuto o del rapporto di lavoro.

Riservatezza

Infine, la invitiamo a mantenere durante lo svolgimento delle mansioni che le sono state affidate e anche dopo la conclusione degli incarichi stessi, la totale riservatezza su tutte le informazioni, siano esse confidenziali e/o riservate di cui è venuto o verrà a conoscenza. Dette informazioni non dovranno essere divulgate a terzi, né in tutto né in parte, né in forma scritta o orale o grafica o su supporto magnetico o in qualsiasi altra forma senza la preventiva espressa autorizzazione del Titolare del trattamento.

Per "informazione confidenziale e/o riservata" si intende qualsiasi informazione, dato, disegno, conoscenza, ritrovato, brevettato o brevettabile, know-how e, in genere, qualsivoglia notizia, di natura tecnica, economica, commerciale o amministrativa, così come qualsiasi disegno, documento, supporto magnetico o campione di materiale o prodotto contrassegnato con la dicitura "riservato" o "confidenziale" o comunque, seppur non contrassegnato, ma identificato anche oralmente come tale dal Titolare del trattamento, che lo trasmette al lavoratore in relazione all'adempimento delle sue mansioni lavorative.

Il Titolare del trattamento CHERASCO PIERGIUSEPPE

CHERASCO SRL

VIA CADUTI SUL DON 38 12020 VILLAR SAN COSTANZO (CN)

VILLAR SAN COSTANZO (CN).....

Il sottoscritto **ING. BIANCO ALBERTO**

prende atto dell'autorizzazione e delle istruzioni contenute nella presente comunicazione e, vista la normativa vigente, **assume** l'incarico **del** trattamento.

VILLAR SAN COSTANZO (CN)_____/_____/20_____