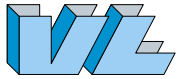


**VERONALAMIERE**  
Technology Service Partner

# ***Modello Organizzativo Privacy (Policy Privacy)***

***Versione di sintesi***

*Rev. 02 – novembre 2023*



## 1. OBIETTIVI E DEFINIZIONI

**Verona Lamiere S.p.A.** si è dotata di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale

Obiettivo del presente documento e di quelli ad esso collegati (conservati in azienda) è definire il **Modello Organizzativo Privacy (Policy Privacy)**, ovvero individuare strategia, linee guida generali e disposizioni interne volte a disciplinare il trattamento dei dati personali effettuato da Verona Lamiere S.p.A., ai sensi del *GDPR – General Data Protection Regulation*.

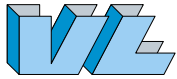
La **politica della privacy (policy)** che discende dal presente Modello Organizzativo Privacy si applica all'azienda nella sua interezza, a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

La sua attuazione è obbligatoria per tutto il personale e deve essere inserita come parte integrante nella regolamentazione di qualsiasi accordo con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nel campo del **Sistema di Gestione della Privacy (SGP)**.

L'azienda Verona Lamiere S.p.A. si impegna a garantire e dimostrare che il trattamento dei dati personali avviene in maniera conforme a quanto previsto dalla normativa e, secondo i seguenti principi di liceità, questi sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui l'azienda Verona Lamiere S.p.A. è Titolare, anche per tutti quei trattamenti di cui l'azienda è nominato Responsabile del trattamento da altri Titolari del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.



Poiché analoghe garanzie di protezione e l'adozione di adeguate misure di sicurezza sono richieste ai soggetti terzi ai quali l'azienda Verona Lamiere S.p.A. affida l'incarico di Responsabile del trattamento, la *policy* in oggetto è resa disponibile presso tali Responsabili del trattamento.

## 2. SICUREZZA DELLE INFORMAZIONI

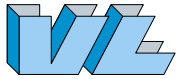
Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali l'azienda assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate. Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo l'azienda ha istituito e mantiene aggiornato un registro delle attività di trattamento.

L'azienda identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi generali, di seguito enunciati:

- Esiste un elenco costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno di essi è individuato un responsabile;
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;
- Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente sottoposte a revisione;
- Sono definite delle procedure per l'utilizzo sicuro dei beni (luoghi, mezzi di trasporto, strumenti) e delle informazioni aziendali;
- È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;



- È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

### 3. RISERVATEZZA DELLE INFORMAZIONI

L'azienda Verona Lamiere S.p.A. si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività in conformità alle procedure interne previste, coerenti con il presente Modello Organizzativo Privacy.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del codice civile.

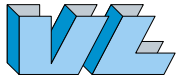
L'azienda si impegna a garantire adeguati livelli minimi di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

### 4. ATTUAZIONE DELLA POLICY

L'osservanza e l'attuazione della politica della privacy (*policy*) che discende dal presente Modello Organizzativo Privacy sono responsabilità di:

- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni che rientrano nel campo di applicazione di sua competenza. Il personale è infatti responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda e che devono garantire il rispetto dei requisiti contenuti nella politica della privacy (*policy*);

Il personale dell'azienda che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno, potrà essere perseguito nelle



opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.

## 5. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

La direzione aziendale verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy, in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

Il Titolare del trattamento, quale responsabile del Sistema di Gestione della Privacy (SGP), ha il compito di condurre operativamente la revisione di questa politica.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy (SGP).

## 6. INFORMAZIONE E FORMAZIONE

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dall'azienda anche e soprattutto grazie alla particolare attenzione alla formazione e alla conoscenza delle modalità di gestione del tema "privacy".

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine dell'azienda. Per gli stessi fini di conoscenza eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

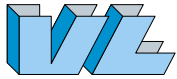
La formazione viene adeguata al proprio sistema di trattamento dei dati personali e in base alla criticità di trattamento eseguita dalla risorsa umana in formazione.

L'azienda riconosce la propria responsabilità che discende dalla normativa vigente e si impegna a proteggere i dati personali che gli utenti affidano ad essa da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di tecnologie e procedure aziendali di protezione secondo le migliori pratiche (*best practices*) di volta in volta disponibili.

## 7. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITA'

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, l'azienda garantisce sempre la precisa individuazione dei soggetti che ricoprono ruoli attivi nel trattamento. Ciò avviene con l'allestimento e il mantenimento efficiente nel tempo di un sistema tracciabile delle nomine e delle relative mansioni.

In questo modo risulta di immediata comprensione la conseguente ripartizione delle responsabilità di ogni soggetto, parametrize alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati ogni volta ritenuto necessario.



Quanto descritto trova riscontro nell'organigramma privacy che viene aggiornato a cadenza periodica ritenuta più opportuna in relazione al settore di attività e all'articolazione della propria organizzazione oppure in occasione di qualsiasi variazione intervenuta.

In accordo con la normativa di riferimento e con la policy che discende dal presente Modello Organizzativo Privacy, costituiscono figure imprescindibili quelle di seguito descritte.

L'azienda Verona Lamiere S.p.A. si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

- diritto all'accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso;
- diritto alla rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- diritto alla cancellazione, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- diritto all'opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, l'azienda Verona Lamiere S.p.A. si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

Contatti del Titolare Trattamento Dati:

**Verona Lamiere S.p.A.**

Via G. Pascoli 46

35179 Zevio (VR)

Alla c.a. del Titolare Trattamento Dati o Ufficio GDPR

E-mail dedicata: [privacy@veronalamiere.it](mailto:privacy@veronalamiere.it)

**La presente policy aziendale GDPR è pubblicata sul sito web <https://www.veronalamiere.it>**