

Modello privacy Pontarolo (MOP)

1. Premessa e Obiettivi

Il presente Modello Organizzativo Privacy (MOP) è stato predisposto dal Gruppo Pontarolo in ottemperanza alle disposizioni del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 (GDPR) e della normativa nazionale vigente in materia di protezione dei dati personali, in particolare il Decreto Legislativo 30 giugno 2003, n. 196, come modificato dal Decreto Legislativo 10 agosto 2018, n. 101.

Il Gruppo Pontarolo, consapevole dell'importanza di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali, si impegna a garantire che ogni attività di trattamento dei dati sia svolta nel pieno rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, nonché del principio di responsabilizzazione (accountability).

Scopo del Modello Organizzativo Privacy

Lo scopo primario di questo MOP è definire e implementare un quadro organico di principi, regole, procedure e misure organizzative, tecniche e di sicurezza volte a garantire la corretta gestione e protezione dei dati personali trattati dal Gruppo Pontarolo. L'obiettivo è assicurare la conformità alle normative sulla privacy, prevenire violazioni dei dati e tutelare i diritti degli interessati.

Il MOP mira inoltre a:

- una chiara definizione di ruoli e responsabilità all'interno del Gruppo in relazione al trattamento dei dati personali;
- implementare processi standardizzati per la raccolta, l'uso, la conservazione e la cancellazione dei dati personali;
- sensibilizzare e formare il personale sull'importanza della protezione dei dati e sulle procedure da adottare;
- una gestione proattiva dei rischi legati al trattamento dei dati personali.

Ambito di Applicazione

Il presente Modello Organizzativo Privacy è **vincolante e trova applicazione** per:

- **tutte le società** che fanno parte del **Gruppo Pontarolo**;
- **tutti i dipendenti, i collaboratori, i tirocinanti e il personale somministrato** che operano per conto del Gruppo Pontarolo;
- **qualsiasi soggetto esterno** (es. fornitori, consulenti, partner) che, a vario titolo, tratti dati personali per conto del Gruppo Pontarolo o nell'ambito di rapporti contrattuali con lo stesso, il quale sarà tenuto al rispetto delle disposizioni del presente Modello e degli accordi specifici stipulati in materia di protezione dei dati.

2. Principi Fondamentali del Trattamento dei Dati

Il Gruppo Pontarolo si impegna ad applicare rigorosamente i principi fondamentali stabiliti dal GDPR per il trattamento dei dati personali, garantendo che ogni operazione sia svolta nel pieno rispetto dei diritti e delle libertà degli interessati. Questi principi rappresentano la base su cui si fonda l'intero sistema di gestione della privacy del Gruppo:

- **Liceità, Correttezza e Trasparenza:** Ogni trattamento di dati personali deve essere svolto in modo **lecito**, basandosi su una valida base giuridica (ad esempio, consenso, esecuzione di un contratto, obbligo legale, interesse legittimo). Il trattamento deve essere condotto in maniera **corretta**, garantendo la protezione e il rispetto degli interessati. Infine, il Gruppo si impegna a essere **trasparente** riguardo alle modalità e alle finalità del trattamento, fornendo informazioni chiare e facilmente accessibili agli interessati.
- **Limitazione della Finalità:** I dati personali sono raccolti per **finalità determinate, esplicite e legittime**, e non sono in seguito trattati in modo incompatibile con tali finalità. Il Gruppo Pontarolo si assicura che le finalità di ogni trattamento siano chiaramente definite e comunicate prima della raccolta dei dati.
- **Minimizzazione dei Dati:** Il trattamento dei dati personali è limitato a quanto **strettamente necessario** rispetto alle finalità per cui sono trattati. Ciò significa che il Gruppo raccoglie solo i dati adeguati, pertinenti e limitati a quanto occorre, evitando la raccolta di informazioni superflue.
- **Esattezza:** I dati personali devono essere **esatti e, se necessario, aggiornati**. Il Gruppo Pontarolo adotta misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti, tenuto conto delle finalità per cui sono trattati.
- **Limitazione della Conservazione:** I dati personali sono conservati in una forma che consente l'identificazione degli interessati per un **periodo di tempo non superiore a quello necessario** al conseguimento delle finalità per le quali sono trattati. Una volta esaurita la finalità o il termine di legge, i dati vengono cancellati o anonimizzati in modo sicuro.
- **Integrità e Riservatezza:** I dati personali sono trattati in modo da garantire un'adeguata **sicurezza**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Il Gruppo implementa misure robuste per proteggere i dati da accessi non autorizzati e per mantenerne l'integrità.
- **Responsabilizzazione (Accountability):** Il Gruppo Pontarolo è **responsabile** del rispetto di tutti i principi sopra elencati ed è in grado di **comprovarli**. Questo principio impone al Titolare del Trattamento di adottare comportamenti proattivi e di dotarsi di tutte le misure organizzative, tecniche e procedurali necessarie a dimostrare la conformità al GDPR. Ciò include la tenuta di registri, la conduzione di valutazioni d'impatto e la formazione del personale.

3. Ruoli e Responsabilità

Per assicurare una gestione efficace e conforme dei dati personali, il **Gruppo Pontarolo** definisce chiaramente i ruoli e le responsabilità di tutti i soggetti coinvolti nel trattamento dei dati. Questa

struttura organizzativa è fondamentale per garantire che ogni attività rispetti i principi del GDPR e le normative applicabili.

Titolare del Trattamento

Il Titolare del Trattamento è l'entità che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Per il Gruppo Pontarolo, in base alla specifica struttura organizzativa e ai flussi di dati, il ruolo di Titolare del Trattamento spetta al Gruppo nel suo complesso: in questo caso, il Gruppo agirà come un unico Titolare, assumendosi la piena responsabilità delle decisioni sul trattamento dei dati.

In particolare, quindi i riferimenti del Titolare del trattamento sono:

Pontarolo Engineering S.p.a.

San Vito Al Tagliamento, 33078, PN, Italia
Via Clauzetto 20
P.IVA 00631040938

Responsabili del Trattamento

I Responsabili del Trattamento sono persone fisiche o giuridiche, autorità pubbliche, servizi o altri organismi che trattano dati personali per conto del Titolare del Trattamento. Il Gruppo Pontarolo si avvale di diversi soggetti esterni per lo svolgimento di specifiche attività (ad esempio, fornitori di servizi IT e cloud, consulenti legali o fiscali, società di gestione paghe).

Con ciascuno di questi soggetti, il Gruppo stipulerà un apposito accordo di nomina a Responsabile del Trattamento, in conformità all'Articolo 28 del GDPR. Tale accordo definirà in modo dettagliato:

- l'oggetto, la durata, la natura e la finalità del trattamento;
- il tipo di dati personali e le categorie di interessati;
- gli obblighi e i diritti del Titolare del Trattamento;
- le istruzioni specifiche del Titolare per il trattamento dei dati;
- gli obblighi del Responsabile in termini di sicurezza dei dati, assistenza al Titolare, notifica dei data breach, restituzione o cancellazione dei dati al termine del trattamento, e messa a disposizione delle informazioni necessarie per dimostrare la conformità.

Soggetti Autorizzati al Trattamento (Incaricati)

All'interno del Gruppo Pontarolo, il Titolare del Trattamento autorizza specifiche persone fisiche a trattare dati personali sotto la propria autorità diretta. Questi soggetti, comunemente definiti Incaricati del Trattamento, sono scelti in base alla loro affidabilità e alle conoscenze necessarie per svolgere le proprie mansioni nel rispetto della privacy.

A ciascun Soggetto Autorizzato saranno impartite istruzioni specifiche e dettagliate sulle modalità del trattamento, le finalità, le misure di sicurezza da adottare e i limiti del proprio operato. Il Gruppo assicurerà che tutto il personale autorizzato riceva una formazione adeguata e periodica in materia di protezione dei dati personali, per garantire che sia pienamente consapevole delle proprie responsabilità e delle procedure da seguire.

Amministratori di Sistema

Gli **Amministratori di Sistema** rivestono un ruolo cruciale nella gestione della sicurezza dei sistemi informativi che trattano dati personali. All'interno del Gruppo Pontarolo, gli Amministratori di Sistema, siano essi interni o esterni, hanno **ruoli e responsabilità specifiche** che saranno dettagliate e

formalizzate. Queste includeranno, a titolo esemplificativo, la gestione degli accessi ai sistemi e ai database, il monitoraggio della sicurezza, l'implementazione di politiche di backup, la gestione delle vulnerabilità e la partecipazione alla risposta agli incidenti di sicurezza.

La loro attività sarà costantemente supervisionata e tracciata, e saranno tenuti a rispettare le politiche di sicurezza del Gruppo e le istruzioni impartite.

L'amministratore di sistema nominato è: Del Re Daniele

4. Gestione dei Trattamenti di Dati Personali

La corretta gestione dei trattamenti di dati personali è il cuore della conformità al GDPR e della tutela della privacy. Il Gruppo Pontarolo adotta un approccio strutturato e proattivo per monitorare, valutare e proteggere i dati in ogni fase del loro ciclo di vita, dalla raccolta alla cancellazione.

Registro delle Attività di Trattamento (Art. 30 GDPR)

Il Gruppo Pontarolo tiene un Registro delle Attività di Trattamento accurato e aggiornato, come previsto dall'Articolo 30 del GDPR. Questo registro è uno strumento essenziale per mappare e documentare tutti i trattamenti di dati personali svolti all'interno del Gruppo. Per ciascuna società che ne fa parte, il registro descrive dettagliatamente:

- le finalità del trattamento;
- le categorie di interessati (es. dipendenti, clienti, fornitori);
- le categorie di dati personali trattati (es. dati anagrafici, dati di contatto, dati particolari);
- le categorie di destinatari a cui i dati sono comunicati;
- i trasferimenti di dati verso paesi terzi o organizzazioni internazionali;
- i termini previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Il Registro è mantenuto in forma scritta elettronica, e viene regolarmente rivisto e aggiornato per riflettere eventuali modifiche nei trattamenti o nell'organizzazione. La responsabilità del mantenimento e dell'aggiornamento ricade sui referenti individuati all'interno di ciascuna società del Gruppo, sotto la supervisione del Titolare del Trattamento e del DPO.

Valutazione d'Impatto sulla Protezione dei Dati (DPIA - Art. 35 GDPR)

Il Gruppo Pontarolo riconosce l'importanza della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) quale strumento proattivo per identificare e mitigare i rischi elevati per i diritti e le libertà delle persone fisiche. La DPIA viene condotta prima di avviare trattamenti che presentano un rischio elevato, ad esempio:

- Trattamenti su larga scala di categorie particolari di dati (es. dati sanitari, biometrici).
- Monitoraggio sistematico su larga scala di aree accessibili al pubblico.
- Valutazioni sistematiche e complete di aspetti personali relative a persone fisiche, basate sulla profilazione o sull'analisi di dati che producono effetti giuridici o significativi simili.
- Utilizzo di nuove tecnologie che possono comportare rischi significativi.

Le procedure per la conduzione della DPIA prevedono:

- Una descrizione sistematica dei trattamenti previsti e delle finalità.
- Una valutazione della necessità e proporzionalità dei trattamenti.
- Una valutazione dei rischi per i diritti e le libertà degli interessati.
- L'identificazione delle misure previste per affrontare tali rischi, comprese le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR.

La DPIA è un processo dinamico che può essere rivisto qualora si verificano cambiamenti significativi nel trattamento.

Misure di Sicurezza Tecniche e Organizzative

Per garantire l'integrità e la riservatezza dei dati, il Gruppo Pontarolo implementa un robusto insieme di misure di sicurezza tecniche e organizzative, volte a proteggere i dati personali da distruzione, perdita, alterazione, divulgazione non autorizzata o accesso accidentale o illecito.

Le misure includono:

- **Misure di sicurezza fisica:** Controllo degli accessi ai locali e alle aree dove sono conservati i dati o i sistemi informativi, mediante sistemi di allarme, videosorveglianza e procedure di accesso limitato al personale autorizzato.
- **Misure di sicurezza logica:** Implementazione di sistemi di **autenticazione** forte (es. username e password complesse, autenticazione a più fattori), **autorizzazione** basata sul principio del minimo privilegio (accesso ai dati solo se strettamente necessario per la mansione), **crittografia** dei dati sensibili e dei dati in transito, e regolari procedure di **backup** per garantire il ripristino dei dati in caso di incidenti.
- **Politiche di password:** Definizione di requisiti rigorosi per la creazione, il cambio periodico e la gestione sicura delle password da parte di tutto il personale.
- **Gestione degli accessi ai sistemi e ai dati:** Implementazione di procedure per l'assegnazione, la modifica e la revoca degli accessi ai sistemi e ai dati, con revisioni periodiche per assicurare che gli accessi siano sempre pertinenti ai ruoli e alle responsabilità.
- **Procedure per la conservazione e la distruzione dei dati:** Definizione di politiche chiare sui tempi di conservazione dei dati, basate sulla finalità e sugli obblighi legali, e procedure sicure per la loro cancellazione o anonimizzazione irreversibile una volta scaduto il termine.
- **Monitoraggio e audit:** Attività regolari di monitoraggio dei sistemi e delle reti per rilevare anomalie o tentativi di accesso non autorizzato. Vengono condotti audit periodici, interni ed esterni, per verificare l'efficacia delle misure di sicurezza e la conformità alle politiche interne e al GDPR.

Gestione delle Violazioni dei Dati Personali (Data Breach - Art. 33-34 GDPR)

Il Gruppo Pontarolo ha stabilito procedure chiare e rapide per la gestione delle violazioni dei dati personali (Data Breach), ovvero eventi che comportano la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati.

Le procedure prevedono:

- **Individuazione e Valutazione:** Sistemi e protocolli per l'identificazione tempestiva di potenziali violazioni, seguita da una rapida valutazione dell'impatto e del rischio per i diritti e le libertà degli interessati.

- **Gestione e Mitigazione:** Azioni immediate per contenere la violazione, mitigare i danni e ripristinare la sicurezza dei sistemi.
- **Comunicazione al Garante:** Se la violazione presenta un rischio per i diritti e le libertà delle persone fisiche, il Gruppo provvede a notificare la violazione all'**Autorità Garante per la Protezione dei Dati Personali** entro 72 ore dal momento in cui ne è venuto a conoscenza.
- **Comunicazione agli Interessati:** Se la violazione è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il Gruppo comunica la violazione anche agli **interessati**, senza ingiustificato ritardo, descrivendo la natura della violazione e le misure adottate per porvi rimedio.

Gestione dei Diritti degli Interessati (Art. 15-22 GDPR)

Il Gruppo Pontarolo garantisce agli interessati la piena possibilità di esercitare i propri diritti in relazione al trattamento dei loro dati personali, in conformità agli articoli 15-22 del GDPR. Sono state definite procedure interne per rispondere in modo tempestivo ed efficace alle richieste relative a:

- **Diritto di accesso:** L'interessato può richiedere conferma dell'esistenza di un trattamento di dati che lo riguarda e ottenere informazioni sui dati trattati e sulle finalità.
- **Diritto di rettifica:** Richiesta di correggere dati personali inesatti o di integrarli se incompleti.
- **Diritto alla cancellazione (diritto all'oblio):** Richiesta di cancellazione dei dati personali in determinate circostanze (es. dati non più necessari per le finalità, revoca del consenso).
- **Diritto di limitazione del trattamento:** Richiesta di limitare il trattamento dei dati a specifiche finalità o per un determinato periodo.
- **Diritto alla portabilità dei dati:** Richiesta di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare.
- **Diritto di opposizione:** Opposizione al trattamento dei dati personali, in particolare per finalità di marketing diretto o basate su interessi legittimi, a meno che non vi siano motivi legittimi cogenti che prevalgono sugli interessi dell'interessato.

Le procedure di gestione delle richieste degli interessati prevedono la verifica dell'identità del richiedente e l'obbligo di fornire una risposta **entro un mese** dalla ricezione della richiesta, prorogabile di ulteriori due mesi in caso di particolare complessità, dandone comunicazione all'interessato.

5. Formazione e Sensibilizzazione

La protezione dei dati personali non è solo un obbligo normativo, ma una **responsabilità condivisa** che coinvolge ogni membro del **Gruppo Pontarolo**. Per questo, un pilastro fondamentale del Modello Organizzativo Privacy è l'impegno costante nella **formazione e sensibilizzazione** del personale. Un'adeguata conoscenza delle normative e delle procedure interne è cruciale per prevenire errori, ridurre i rischi e garantire un comportamento proattivo e consapevole nella gestione quotidiana dei dati.

6. Controlli e Revisione

Un Modello Organizzativo Privacy efficace non è un documento statico, ma un sistema dinamico che richiede **monitoraggio continuo e aggiornamenti regolari**. Il **Gruppo Pontarolo** si impegna a verificare costantemente l'adeguatezza e l'efficacia del presente MOP, garantendo che rimanga allineato alle esigenze operative del Gruppo, alle evoluzioni tecnologiche e agli aggiornamenti normativi. Questo

approccio proattivo è essenziale per mantenere un elevato livello di protezione dei dati personali nel tempo.

Per assicurare la conformità e l'efficacia del MOP, il Gruppo Pontarolo implementa diverse **modalità di verifica e audit interno**. Queste attività sono progettate per identificare tempestivamente eventuali lacune, non conformità o aree di miglioramento.

Il MOP è soggetto a un processo di **aggiornamento e miglioramento continuo**. Il processo di aggiornamento prevede la revisione periodica del MOP (almeno una volta all'anno o con maggiore frequenza in caso di eventi significativi), l'integrazione di nuove procedure o la modifica di quelle esistenti, e la successiva comunicazione al personale interessato. L'obiettivo è mantenere il Modello Organizzativo Privacy un riferimento vivo e attuale per la gestione della protezione dei dati all'interno del Gruppo Pontarolo.