Etica, integrità, responsabilità sociale, tutela dell'ambiente, sostegno alla comunità, innovazione, inclusione, diversità, equità, eccellenza dei propri servizi, sono i Valori che Off. Mara ritiene di porre alla base delle relazioni con i suoi portatori di interesse. Vogliamo essere riconosciuti come soggetti in grado di ispirare fiducia e guidare il cambiamento, rispondendo alle aspettative che i nostri clienti e la comunità hanno verso di noi. Grazie ai nostri Valori, ci impegnano ad agire nel rispetto di tutte le norme di legge e delle buone pratiche organizzative e gestionali, promuovendo il miglioramento continuo.
È per questo che OFF. MARA adotta strumenti organizzativi volti a gestire, attraverso criteri risk based, aspetti quali: qualità, sicurezza del prodotto, tutela dell'ambiente, della privacy, salute e sicurezza sul lavoro, responsabilità sociale d'impresa e prevenzione della corruzione, diversità, inclusione ed equità, considerando le best practice di riferimento.
La sottoscrizione del presente documento di Politica Integrata sancisce l'impegno a darne piena attuazione e a renderlo disponibile a tutte le parti interessate. OFF. MARA si impegna a contrastare attraverso gli strumenti a disposizione ogni comportamento contrario ai principi ispiratori della presente Politica e ad aggiornarne i contenuti in relazione alle evoluzioni normative e alla strategia aziendale.
La Politica Aziendale si ispira ai seguenti principi:

- Il ruolo centrale della Direzione Aziendale.
- Il forte orientamento al Cliente.
- La cultura della qualità a tutti i livelli organizzativi.
- Il miglioramento continuo.
- L'attenzione agli stakeholder, con particolare riguardo alle risorse umane, vero patrimonio aziendale.
- L'analisi del contesto in cui si opera e la consapevolezza dei rischi e delle opportunità associate.
- La comunicazione interna ed esterna.

I principi sovra menzionati vengono perseguiti dalla nostra Organizzazione tramite la definizione e applicazione dei seguenti indirizzi, quadro di riferimento per l'individuazione degli obiettivi.

**1. Qualità delle lavorazioni e attenzione al Cliente:** Off.Mara, con il diretto impegno della Direzione, sviluppa le proprie lavorazioni in conformità a leggi, alle norme, standard tecnici nazionali e internazionali, proponendo un'immagine aziendale interattiva che permetta di offrire in modo originale e trasparente i propri servizi.

**2. Determinazione delle esigenze e aspettative delle parti interessate:** l'identificazione dell'insieme degli interlocutori interni (tra cui i lavoratori) ed esterni (tra cui i Clienti) e l'analisi delle relative esigenze e aspettative rappresenta un momento cruciale per la corretta pianificazione del sistema di gestione, in particolare per la definizione di idonee strategie aziendali. I requisiti dei Clienti vengono analizzati dettagliatamente per garantire il pieno soddisfacimento delle relative aspettative e garantendo il libero accesso ai clienti e alle autorità che ne facessero richiesta.

**3. Analisi del contesto, dei rischi e delle opportunità:** In particolare Off. Mara, tenendo conto del proprio contesto di riferimento si impegna a sviluppare, a mantenere attivi e a migliorare i propri strumenti per la Gestione per la Qualità divulgando, all'interno della propria organizzazione e tra tutte le parti interessate, l'importanza di rispettare i requisiti ad essa applicabili, attendendosi alle disposizioni di legge e dalle best practice di riferimento, sempre considerando le aspettative del cliente. L'Organizzazione utilizza il Risk based Thinking come strumento strategico per la consapevolezza ed il controllo, finalizzato sia alla mitigazione di tutti i rischi aziendali sia alla individuazione e al consolidamento di opportunità di mercato e di miglioramento dei risultati e dei processi.

**4. Ottimizzazione struttura organizzativa, analisi e monitoraggio:** la determinazione dei singoli processi, delle interazioni fra gli stessi e l'identificazione delle responsabilità relative a ogni processo è alla base della nostra filosofia aziendale, al fine di ottimizzare i processi decisionali e le attività conseguenti, monitorando le performance aziendali, attraverso l'analisi dei dati e delle informazioni raccolte.

**5. Coinvolgimento del personale, competenza e consapevolezza:** Off. Mara si impegna a rendere disponibili le risorse necessarie ad assicurare, in coerenza con gli obiettivi definiti, che ogni singola persona si senta una parte indispensabile dell'azienda, comprendendo l'importanza di ciascuna attività affidata, nonché del rispetto delle norme ambientali, di salute e sicurezza. Ogni lavoratore deve essere messo in condizione di eseguire i compiti affidati attraverso un processo di partecipazione e continuo coinvolgimento, anche tramite attività di formazione ed addestramento, garantendo il mantenimento di un comportamento etico a tutti i livelli organizzativi.

**6. Rapporto di reciproco beneficio con i fornitori:** solo una continua collaborazione con i fornitori può permettere il raggiungimento di obiettivi condivisi, volti al conseguimento della soddisfazione dei Clienti, garantendo la sostenibilità economica.

**7. Dotazione infrastrutturale:** Off. Mara si impegna ad utilizzare le migliori tecnologie disponibili sia hardware che software, coerentemente alle disponibilità economiche, per l'erogazione dei propri servizi al fine di minimizzare potenziali impatti negativi sui requisiti di riservatezza delle proprietà intellettuali dei Clienti e dei fornitori, sulla salute e sicurezza dei lavoratori e sull'efficienza aziendale.

**8. Comunicazione:** Off.Mara si impegna ad assicurare flussi comunicativi, interni ed esterni, al fine di fornire informazioni chiare, trasparenti, comprensibili e allineate agli obiettivi comunicativi; una corretta comunicazione contribuisce a creare valore per l'azienda, consentendo di rispondere in modo adeguato alle esigenze ed alle aspettative delle parti interessate.

**9.** **Massima attenzione agli aspetti salute-sicurezza:** Off. Mara crede fermamente nella necessità di garantire un ambiente di lavoro salubre e sicuro per tutti i collaboratori aziendali, mettendo a disposizioni macchinari dotati di elevati standard di sicurezza, attuando opportune misure tecnico-procedurali e assicurando la consultazione, partecipazione e responsabilizzazione dei dipendenti, nell'ambito delle proprie mansioni, in merito al processo di salvaguardia della salute, della sicurezza e dell'incolumità pubblica; a tal fine vengono sviluppati programmi di miglioramento continuo per raggiungere sempre più elevati standard di salute e sicurezza e livelli ergonomici diffusi. Prevenire eventi incidentali, infortuni e malattie professionali.

**10.** **Minimizzazione degli impatti ambientali negativi**: Off. Mara è impegnata a soddisfare i requisiti legali nonché gli eventuali altri requisiti ad essa applicabili, anche volontariamente sottoscritti e utili a mantenere e a migliorare nel tempo le proprie prestazioni ambientali. Off. Mara si impegna ad adottare opportuni accorgimenti per prevenire sprechi di risorse naturali ed energetiche, mitigare le emissioni in atmosfera in termini di tonnellate di Co2 equivalente e minimizzare nonché la produzione di rifiuti nel corso dello svolgimento delle attività produttive garantendone l'idoneo smaltimento.

**11.** **Minimizzazione dei rischi relativi alla gestione dei dati personali:** Off. Mara si impegna a garantire l'applicazione dei principi di trasparenza e responsabilità sanciti dal Reg. UE 2016/679: a supporto di tale impegno è stata definita una specifica Policy, parte integrante della presente Politica Integrata (All. A "Policy Aziendale in materia di protezione dei dati personali").

Off.Mara ha definito i propri processi aziendali, identificando ruoli e responsabilità per garantire il perseguimento degli indirizzi sovra enunciati. La Direzione si impegna a raggiungere i risultati prefissati anche mediante la definizione e la formalizzazione, a cadenze variabili, di obiettivi specifici misurabili per ogni livello, funzione e processo ritenuto strategico dell'Organizzazione.

La politica, in sede di riunioni di riesame, è oggetto di analisi per accertarne la continua idoneità e per garantire che:

- sia appropriata alla "missione" dell'azienda;
- sia allineata sempre al contesto dell'organizzazione;
- costituisca un quadro di riferimento per fissare gli obiettivi nei vari ambiti di applicazione comprenda l'impegno a soddisfare i requisiti applicabili in tema di tutela dell'ambiente e salute e sicurezza dei lavoratori, al soddisfacimento dei requisiti qualitativi e di sicurezza del prodotto, al miglioramento continuo e alla prevenzione;
- preveda la definizione di specifici obiettivi di miglioramento qualità, ambientali e per la sicurezza, coerenti con la politica e soggetti a misurazione e riesame;
- sia diffusa a tutte le parti esterne interessate (es Autorità di controllo, clienti, fornitori, pubblico);
- sia diffusa e compresa da tutti i collaboratori dell'azienda.

La politica è stata:

- esposta all'interno dei locali per permetterne la visione anche ai visitatori;
- resa disponibile in rete attraverso il sistema informatico;
- resa disponibile sul sito internet aziendale

Diffusione della Politica Integrata

L'Amministratore Unico, consapevole che la Politica Aziendale debba essere compresa, attuata e sostenuta a tutti i livelli dell'Organizzazione, fornisce adeguata informazione a tutto il personale anche mediante:

- incontri specifici tra la Direzione ed il personale;
- la pubblicazione/distribuzione di estratti.

Il grado di comprensione della politica viene verificato nel corso degli audit interni e mediante incontri del personale con il Responsabile del Sistema di Gestione.

L'Amministratore Unico

Gianni Mara

ALLEGATO A

# Policy aziendale
# in materia di protezione dei dati personali
# Reg. (UE) 679/201

AVVERTENZE

Il contenuto del presente documento rappresenta in dettaglio la policy Implementata relativa al Regolamento (UE) 2016/679 in osservanza ai principi di trasparenza e responsabilità da quest'ultimo sanciti.
Il documento viene verificato periodicamente per mantenere la validità e l'efficacia nel corso del tempo.
Nessun elemento di questo documento può essere distribuito, duplicato o riprodotto anche parzialmente per utilizzi di terze parti senza il preventivo consenso scritto del Titolare di OFF. MECCANICA DI MARA GIANMARIO & C. S.R.L. In violazione di quanto prescritto, la Società si riserva il ricorso alle sedi giudiziarie opportune per la tutela della propria organizzazione e reputazione nonché per il rispetto dei principi di riservatezza e confidenzialità richiamati dall'ordinamento giuridico nazionale ed europeo.

**Sommario**

1) Premessa 2
1.1) Oggetto e scopo 2
1.2) Contesto normativo di riferimento 2
1.3) Principi generali 3
1.4) Adozione e aggiornamento 3
1.5) Definizioni 3
1.6) Ambito di applicazione 5
2) Ruoli privacy 5
2.2) Soggetti autorizzati al Trattamento 5
2.3) Responsabili del Trattamento (Artt. 27 e 28 GDPR) 5
2.4) Amministratore di Sistema (Provv. Autorità Garante Privacy del 27 novembre 2008) 6
3) Gestione dei trattamenti 7
3.1) Condizioni di liceità del trattamento (Artt. 5 e 6 GDPR) 7
3.2) Trattamento di dati di minori e di categorie particolari di dati personali (Artt. 8 e 9 GDPR) 7
3.3) Cautele da adottare da parte dell'Incaricato 7
3.4) Gestione del Registro dei trattamenti (Art. 30 GDPR) 8
4) Principi di protezione dei dati personali 8
4.1) Accountability (Art. 5 GDPR) 8
4.2) Privacy by design (Art. 25 GDPR) 8
4.3) Privacy by default (Art. 25 GDPR) 8
5) Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali (Artt. 44, 45 e 46 GDPR) 9
6) Diritti degli interessati 9
6.1) I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR) 9
6.2) I diritti non subordinati a una richiesta dell'interessato 9
7) Misure di sicurezza (Art. 32 GDPR) 10
8) La valutazione d'impatto sulla protezione dei dati personali – DPIA (Art. 32 GDPR) 10
9) Data breach (Artt. 33 e 34 GDPR) 11

10) Il sistema delle relazioni e dei flussi informativi 11

11) Allegati 12

## 1) Premessa

### 1.1) Oggetto e scopo

La presente Policy sulla Protezione dei Dati Personali (la "Policy") definisce le linee guida alle quali la Società OFF. MECCANICA DI MARA GIANMARIO & C. S.R.L. (di seguito denominata "Titolare") deve attenersi nella pianificazione e nello svolgimento di qualsivoglia attività che implichi il trattamento di Dati personali per assicurare la tutela di tali Dati secondo i requisiti previsti dalla normativa in materia e in particolare al Regolamento (UE) 2016/679 in materia di protezione dei Dati personali (di seguito anche "GDPR").
Le disposizioni della presente Policy hanno il fine di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche.
In particolare, la Policy individua:

- destinatari della normativa interna ed esterna in materia di privacy;
- i principi generali a protezione dei Dati personali a cui è improntata l'attività della Società;
- le modalità di aggiornamento e revisione della Policy;
- i principali ruoli previsti in ambito privacy;
- i processi sottesi a pianificazione e svolgimento di attività del Titolare che implicano il trattamento di Dati personali.

### 1.2) Contesto normativo di riferimento

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato il Regolamento UE n. 679/2016 in materia di protezione dei Dati personali (di seguito "GDPR" e "Regolamento"), entrato in vigore il 25 Maggio 2016 e direttamente applicabile in tutta l'Unione Europea dal 25 Maggio 2018 con conseguente abrogazione della Direttiva 95/46/CE del Parlamento e del Consiglio Europeo del 24 Ottobre 1995, recepita in Italia dal Decreto Legislativo n. 196 del 30 Giugno 2003 (Codice in materia di protezione dei Dati personali) e novellata dal Decreto Legislativo n. 101 del 10 agosto 2018 recate Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati personali.

Il GDPR modifica in maniera profonda la normativa in materia di privacy e in particolare:

- armonizza la disciplina sulla protezione dei Dati personali all'interno di tutta l'Unione europea;
- attribuisce fondamentale importanza ai principi della accountability, della privacy by design e by default;
- coerentemente con il principio della accountability, introduce, inter alia, gli istituti del Registro dei trattamenti, della valutazione d'impatto sulla protezione dei dati e della data breach notification;
- rafforza e introduce nuovi diritti degli interessati, che le imprese sono tenute a garantire al fine di assicurare che il trattamento dei Dati personali sia svolto in piena conformità alla normativa, anche per incrementare il livello dei servizi forniti ai clienti;
- introduce la figura del Data Protection Officer;
- inasprisce le sanzioni amministrative pecuniarie che, nei casi delle violazioni ritenute più gravi, possono arrivare sino ad un massimo di 20.000.000€ o al 4% del fatturato globale annuo a livello di gruppo imprenditoriale.

Il contesto normativo di riferimento comprende inoltre l'ulteriore normativa primaria e secondaria in materia privacy e protezione dei Dati personali, compresi i provvedimenti emanati dal Garante, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

### 1.3) Principi generali

Il Titolare svolge le proprie attività nel rispetto dei principi generali in materia di privacy previsti dalla normativa di riferimento e dalla presente Policy.
In particolare, nella pianificazione o espletamento di qualsiasi attività che comporti trattamento di Dati personali, il Titolare assicura che i Dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**);

- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità (**principio di limitazione della finalità**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**principio di minimizzazione dei Dati personali**);
- esatti e, se necessario, aggiornati tempestivamente rispetto alle finalità per le quali sono trattati (**principio di esattezza**);
- 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 (**principio di limitazione della conservazione**);
- 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 (**principi di integrità e riservatezza).**

**1.4) Adozione e aggiornamento**

Il Titolare del trattamento di OFF. MECCANICA DI MARA GIANMARIO & C. S.R.L. per quanto di competenza, effettua i controlli necessari a verificare l'effettivo rispetto della presente Policy.

**1.5) Definizioni**

Ai fini della presente Policy si intende per:

- "**Categorie particolari di Dati personali**": Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona – articolo 9 GDPR;
- "**Data breach**": 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; in caso di violazione dei Dati
  personali, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, salvo che sia improbabile che tale violazione presenti un rischio per i
  diritti e le libertà delle persone fisiche. Quando la violazione dei Dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione anche all'interessato senza ingiustificato ritardo;
- "**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 – articolo 4, punto 1), GDPR;
- "**Data Protection Officer o DPO**": indica il soggetto designato dal Titolare o dal Responsabile del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR;
- "**Garante**": l'Autorità garante italiana per la protezione dei Dati personali;
- "Incaricato": la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- "**Limitazione di trattamento**": il contrassegno dei Dati personali conservati con l'obiettivo di limitarne il trattamento in futuro – articolo 4, punto 3), GDPR;
- "**Principio di accountability**": il principio che impone al titolare di mettere in atto le misure tecniche e organizzative adeguate per garantire e per dimostrare che il trattamento è effettuato conformemente alle disposizioni del GDPR tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;
- "**Principio di privacy by default**": il principio che richiede al titolare di predisporre misure tecniche e organizzative tali da garantire che, per impostazione predefinita, siano trattati esclusivamente i Dati personali necessari a ogni specifica finalità del trattamento, ad esempio riducendo la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione e il numero di soggetti che ha accesso ai Dati personali;
- "**Principio di privacy by design**": il principio che prescrive al titolare di adottare sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso misure tecniche e organizzative adeguate a garantire il rispetto del GDPR e la tutela dei diritti e delle libertà degli interessati;

- **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 – articolo 4, punto 4), GDPR;
- "**Procedura**": il documento adottato dal Titolare al fine di disciplinare specifici processi interni;
- "**Referente privacy**": il soggetto interno alla Società del Titolare che supporta il DPO nello svolgimento delle sue funzioni.
- "**Registro dei trattamenti**": i titolari e i Responsabili del trattamento devono tenere il registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni di cui all'articolo 30 GDPR;
- "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 – articolo 4, punto 8), GDPR;
- "**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 – articolo 4, punto 7), GDPR. Ai fini della presente Policy, il Titolare del trattamento coincide con OFF. MECCANICA DI MARA GIANMARIO & C. S.R.L.
- "**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 – articolo 4, punto 2), GDPR;
- "**Valutazione di impatto sulla protezione dei dati**" o "Data Protection Impact Assessment (DPIA)": valutazione di impatto sulla protezione dei dati effettuata dal titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- "**WP29**": organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei Dati personali designate da ciascuno Stato membro dell'Unione Europea costituito ai sensi dell'articolo 29 della Direttiva CE 95/46.

### 1.6) Ambito di applicazione

Tutto il personale dipendente, i consulenti con contratto di collaborazione coordinata e continuativa, i collaboratori esterni occasionali, gli addetti alla manutenzione dei sistemi IT, gli stagisti e gli ulteriori collaboratori del Titolare a diverso titolo, ed i partner esterni che hanno accesso per contratto alle basi dati, in qualità di Responsabili del trattamento esterno (ex art. 28) sono tenuti a rispettare scrupolosamente la presente Policy nell'ambito delle rispettive competenze e attività.
Al fine di assicurare a tutti i destinatari la conoscenza dei principi, degli indirizzi e delle procedure adottati dal Titolare in conformità alla presente Policy, la stessa e i relativi aggiornamenti sono pubblicati nel set Documentale privacy.

## 2) Ruoli privacy

### 2.1) Referente privacy

Il Referente Privacy, se previsto, è nominato dal Titolare del trattamento in funzione dell'esperienza professionale, delle competenze specialistiche in materia di protezione dei Dati personali nonché della conoscenza del business della Società .
Il Referente privacy svolge un ruolo di collegamento tra il DPO (ove nominato), gli Incaricati ed il Titolare e collabora con il DPO svolgendo le attività dettagliate nell'**allegato 2** alla presente Policy.

### 2.2) Soggetti autorizzati al Trattamento

Il Titolare adotta delle procedure interne per la nomina ad Incaricati delle persone fisiche dallo stesso autorizzate a trattare Dati personali e per l'aggiornamento di tali nomine.
Il processo di nomina è disciplinato all'interno dell'apposita Procedura aggiornata e pubblicata nel Documentale.
Il Titolare garantisce inoltre un'adeguata formazione degli Incaricati tramite corsi e la fornitura di istruzioni precise su come effettuare i trattamenti. A tal fine, il Titolare organizza eventi di formazione in materia di protezione dei Dati personali, sulla normativa applicabile e sull'impianto privacy adottato. Questi eventi formativi sono organizzati periodicamente e, in ogni caso, qualora dovessero intervenire novità normative o organizzative rilevanti.

**2.3) Responsabili del Trattamento (Artt. 27 e 28 GDPR)**

Il Titolare può esternalizzare alcuni trattamenti a soggetti individuati quali Responsabili del trattamento, selezionati tenendo in considerazione la capacità di offrire garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate al rispetto dei requisiti del GDPR.

Ogni qualvolta un trattamento è esternalizzato ad una persona fisica o giuridica, il Titolare assicura che tale soggetto terzo sia nominato Responsabile esterno del trattamento nel rispetto delle disposizioni del GDPR.

Una volta selezionato il Responsabile esterno nel rispetto della presente Policy, si provvede alla sottoscrizione di un contratto o diverso atto giuridico di nomina che presenti tutti gli elementi richiesti dal GDPR, tra cui precise istruzioni cui il Responsabile esterno dovrà attenersi e il diritto del Titolare di risolvere il contratto in caso di inadempimento della controparte.

Nel corso di tutta la relazione contrattuale, è assicurato un continuo monitoraggio, tramite verifiche periodiche sull'operato dei Responsabili esterni al fine di appurare il rispetto della normativa in materia di privacy e delle istruzioni impartite dal Titolare.

A tal fine, potrà essere sollecitato l'invio di rendiconti, la compilazione di questionari e/o potranno essere effettuate delle visite ispettive presso il Responsabile esterno anche coinvolgendo, qualora necessario, esperti in materia informatica.

Nel caso in cui emergessero criticità, è coinvolto il DPO (ove nominato), insieme al Titolare del trattamento, per valutare interventi per la loro mitigazione. Qualora le criticità dovessero perdurare o fossero di un'entità tale da giustificare la cessazione del rapporto contrattuale, il Titolare interrompe la relazione contrattuale con il Responsabile esterno.

In caso di nomina di un nuovo Responsabile esterno o di modifica di Responsabili esterni esistenti, deve essere aggiornato conseguentemente anche il Registro dei trattamenti.

I dettagli operativi per la gestione dei Responsabili esterni sono descritti e/o monitorati all'interno della Società dal Titolare del trattamento.

**2.4) Amministratore di Sistema (Provv. Autorità Garante Privacy del 27 novembre 2008)**

Il Titolare individua una figura professionale, dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi
di dati, i sistemi operativi, le configurazioni hardware, la profilazione di accesso ai sistemi, le modalità di salvataggio dei dati, ed altre procedure utilizzate dalla Società, le reti locali e gli apparati di sicurezza, nella
misura in cui consentano di intervenire sui dati personali.

In sintesi, i compiti dell'Amministratore di sistema previsti sono:

a) organizzare e gestire il sistema di autenticazione informatica realizzato, se del caso, in Microsoft Active Directory, tenendo conto dell'ambito di trattamento consentito ai singoli operatori. In particolare:
   - generare, sostituire ed invalidare, se necessario, le parole chiave ed i codici identificativi personali da assegnare agli autorizzati al trattamento dati sulla base delle indicazioni fornite dal Titolare.
   - procedere all'immediata disattivazione dei codici identificativi personali in caso di perdita della qualità che consentiva all'utente l'accesso all'elaboratore (ad esempio, cambio mansione, cessazione del rapporto di lavoro/collaborazione) sulla base delle indicazioni fornite dal Titolare, oppure nel caso di mancato utilizzo dei medesimi codici per oltre 6 (sei) mesi;
b) fornire al Titolare indicazioni per l'adozione di programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima sicurezza dei sistemi utilizzati e dei dati ivi presenti.
c) predisporre e rendere funzionante un sistema di backup dei dati e delle applicazioni, verificando periodicamente la validità dei salvataggi effettuati. Laddove non presente come soluzione fornita presso terzi.
d) predisporre un sistema di ripristino che consenta alla Società di tornare alla piena operatività nelle 24 ore successive al verificarsi di eventi dannosi;
e) risolvere eventuali problematiche hardware/software che coinvolgano il server, i client e le altre apparecchiature informatiche in uso alla Società e testare funzionalità e resilienza dei sistemi impiegati;
f) gestire la rete lan, le e-mail della Società, gli accessi remoti ai server;
g) segnalare al titolare ed eventualmente rimuovere, su sua indicazione, software privi di licenza installati sui dispositivi in uso agli autorizzati al trattamento e, in generale, a tutti gli operatori;
h) predisporre un piano di controlli periodici, da eseguire con cadenza semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate dalla Società;
i) collaborare con il Titolare per l'attuazione delle prescrizioni eventualmente impartite dal Garante.
j) non procedere alla modifica, alla cancellazione, alla distruzione o alla perdita di dati nonché al compimento di qualsiasi operazione di trattamento che non sia espressamente autorizzata;

**Registrazione degli accessi dell'Amministratore di sistema**

Qualora nello svolgimento delle attività l'Amministratore di sistema operi su sistemi allocati presso la propria sede e/o presso sedi di soggetti terzi (diversi dal Titolare del trattamento), L' Amministratore di sistema, assicura

l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

## 3) Gestione dei trattamenti

### 3.1) Condizioni di liceità del trattamento (Artt. 5 e 6 GDPR)

Il Titolare garantisce che i Dati personali siano trattati esclusivamente in presenza di una delle condizioni di liceità del trattamento previste dal GDPR, tenendo in considerazione la natura del dato personale oggetto di trattamento (i.e. dati comuni, categorie particolari di Dati personali, dati giudiziari e dati di minori).
In particolare, il Titolare adotta i presidi necessari ad assicurare che il trattamento di Dati personali sia effettuato solo ove ricorra almeno una delle seguenti condizioni:

- l'interessato ha espresso il proprio consenso;
- il trattamento è necessario per eseguire un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per perseguire un legittimo interesse del titolare o di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

Nel dare avvio a una nuova tipologia di trattamento, il Titolare verifica con il coinvolgimento del DPO (ove nominato), che esso sia fondato su una delle fonti di liceità del trattamento di cui sopra.
Il Titolare fornisce agli Incaricati che interagiscono con gli interessati le istruzioni necessarie a garantire il rispetto della normativa e della presente Policy.
Qualora il fondamento di liceità del trattamento sia il consenso, gli Incaricati devono rilasciare un'informativa agli interessati e richiedere il consenso, nel rispetto delle procedure interne e delle istruzioni ricevute, prima che il trattamento abbia inizio. Il consenso deve essere libero, specifico e informato, manifestato tramite un'azione positiva inequivocabile e richiesto separatamente per ogni finalità del trattamento.
Le disposizioni interne stabiliscono l'obbligo di registrare l'ottenuto consenso mediante procedure che assicurino un agevole recupero di data, modalità e contenuto del consenso.
I termini del trattamento, indicati sulle informative, contengono e descrivono in modo puntuale il periodo di conservazione dei Dati personali oppure, se non possibile, i criteri utilizzati per determinare tale periodo.

### 3.2) Trattamento di dati di minori e di categorie particolari di dati personali (Artt. 8 e 9 GDPR)

Nel caso in cui il trattamento sia basato sul consenso e abbia ad oggetto Dati personali di minori, il Titolare assicura che il trattamento abbia luogo esclusivamente se tale consenso è prestato o autorizzato dal titolare della potestà genitoriale.
Il consenso o l'autorizzazione del titolare della responsabilità genitoriale sono registrati tramite processi che ne assicurino un agevole recupero.
Qualora il trattamento riguardi Categorie particolari di Dati personali e il trattamento si basi sul consenso, il Titolare assicura che sia rilasciata un'informativa agli interessati e richiesto un consenso esplicito, nel rispetto delle Procedure interne, prima che il trattamento abbia inizio.

### 3.3) Cautele da adottare da parte dell'Incaricato

La permanenza di atti e documenti cartacei presso l'Incaricato deve essere limitata al tempo strettamente necessario per eseguire le operazioni di trattamento; al termine dell'attività la documentazione deve essere riposta nel rispettivo archivio.
Nel caso di documenti in output (si intendono come tali i documenti o i supporti contenenti Dati personali prodotti e rilasciati dalla struttura a soggetti esterni alla struttura stessa) è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo.
L'Incaricato deve trattare qualunque prodotto dell'elaborazione di Dati personali, anche se non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla versione definitiva. A tal proposito, il Titolare del trattamento ha prodotto e diffuso specifiche codici di condotta denominate: Clear desk Policy, Data retention Policy consultabili a richiesta.

### 3.4) Gestione del Registro dei trattamenti (Art. 30 GDPR)

Il Titolare gestisce la tenuta, l'aggiornamento e la conservazione del Registro dei trattamenti nel rispetto della normativa e della presente Policy.

Le funzioni della Società coinvolgono il Referente privacy in fase di valutazione di attività che potrebbero comportare una modifica o istituzione di un trattamento e l'eventuale necessità di aggiornare il Registro dei trattamenti, tra cui a titolo esemplificativo:

- la progettazione di una nuova iniziativa che preveda il trattamento di Dati personali;
- l'estensione di un trattamento già previsto a nuove categorie di interessati o Dati personali;
- qualsiasi modifica della struttura organizzativa della società;
- la sottoscrizione di contratti di fornitura che comportino la nomina a Responsabile esterno della controparte;
- le categorie di destinatari cui i Dati personali oggetto del trattamento sono comunicati;
- la necessità di trasferire i Dati personali trattati all'esterno dell'Unione europea;
- qualsiasi modifica dei sistemi informativi adottati;
- l'adozione di nuove misure tecniche e/o organizzative.

Il Registro dei trattamenti aggiornato deve essere reso disponibile a tutti gli Incaricati del Titolare secondo modalità atte ad assicurarne l'agevole consultazione.

## 4) Principi di protezione dei dati personali

### 4.1) Accountability (Art. 5 GDPR)

Per trattare i Dati personali in conformità con la normativa vigente e la presente Policy, il Titolare adotta misure tecniche, organizzative e di sicurezza adeguate, nonché adeguati meccanismi di controllo della costante conformità ti tali misure nel tempo e ne dispone il costante aggiornamento.
Il Titolare documenta le attività svolte per garantire che i trattamenti siano effettuati in conformità alla normativa applicabile e tiene tale documentazione a disposizione per eventuali accessi del Garante.

### 4.2) Privacy by design (Art. 25 GDPR)

Il Titolare assicura che tutte le applicazioni, servizi, prodotti ed attività che prevedono il trattamento di Dati personali siano progettati e successivamente effettuati tenendo in considerazione gli effetti che potrebbero avere sulla protezione dei Dati personali e sui diritti degli interessati. A tal fine, sin dal momento della determinazione di modalità e mezzi del trattamento dei Dati personali, sono adottate misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione dei dati, volte ad attuare in modo efficace i principi di protezione dei Dati e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti della normativa applicabile e a tutelare i diritti degli interessati.

### 4.3) Privacy by default (Art. 25 GDPR)

Il Titolare assicura che siano trattati, per impostazione predefinita, esclusivamente i Dati personali necessari per ogni specifica finalità del trattamento.
A tal fine, in fase di delineazione del trattamento, sono adottate le idonee misure tecniche e organizzative e sono valutati, in particolare, i seguenti elementi allo scopo di ridurre al minimo necessario l'impatto sul diritto alla protezione dei Dati personali rispetto alle finalità perseguite:

- quantità dei Dati personali da raccogliere;
- portata del trattamento;
- periodo di conservazione;
- numero di soggetti che ha accesso ai Dati personali.

## 5) Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali (Artt. 44, 45 e 46 GDPR)

Il trasferimento di Dati personali all'esterno dell'Unione Europea può avvenire, in presenza di almeno una delle seguenti condizioni:

- una decisione di adeguatezza della Commissione Europea;
- clausole tipo di protezione ("Model Contract Clauses") dei dati adottate dalla Commissione Europea;
- clausole contrattuali tra il Titolare del trattamento e il Titolare/Responsabile destinatario dei Dati personali nel paese terzo approvate dall'autorità di controllo;
- adozione di un codice di condotta o meccanismo di certificazione e contestuale impegno del Titolare/Responsabile destinatario dei Dati personali di applicare le garanzie adeguate.

Il trasferimento di Dati personali verso un paese terzo o un'organizzazione internazionale sarà inoltre possibile nel caso in cui:

- l'interessato abbia prestato esplicitamente il consenso dopo essere stato informato dei possibili rischi;

- il trasferimento sia necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare ovvero di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

## 6) Diritti degli interessati

I diritti attribuiti dal GDPR agli interessati si dividono in due categorie: (i) i diritti che necessitano di una richiesta espressa dell'interessato; (ii) i diritti ai quali la normativa collega un obbligo del titolare in modo autonomo dalla ricezione di una previa richiesta dell'interessato.

### 6.1) I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR)

Il processo per la gestione dei diritti esercitati dagli interessati mediante espressa richiesta è riconducibile alle seguenti fasi principali:

- ricezione della richiesta;
- gestione della richiesta;
- riscontro all'interessato e archiviazione.

I principali diritti che il GDPR garantisce all'interessato e che lo stesso può esercitare mediante richiesta sono i seguenti:

1. **Diritto di Accesso**. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di Dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai Dati personali che comprendono i Dati personali conferiti dall'interessato i Dati personali osservabili generati in esecuzione del contratto, i termini del trattamento compreso il periodo di conservazione previsto.
**2. Diritto di Rettifica**. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei Dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei Dati personali incompleti, anche fornendo una dichiarazione integrativa;
**3. Diritto di Cancellazione**. L'interessato ha il diritto di ottenere dal titolare del trattamento, se sussistono i motivi indicati dal GDPR, la cancellazione dei Dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i Dati personali;
**4. Diritto di limitazione di trattamento**. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando si verificano le ipotesi previste dall'art. 18 del GDPR;
**5. Diritto di Opposizione / Revoca**. L'interessato ha il diritto di opporsi, o revocare il consenso, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei Dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i Dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà
dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
**6. Diritto alla Portabilità**. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali Dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento sia effettuato con mezzi automatizzati.
Infine, nel caso di esercizio dei diritti di rettifica, cancellazione e/o limitazione del trattamento da parte dell'interessato, il Titolare provvede anche a effettuare la comunicazione ai destinatari interessati prevista dall'articolo 19 GDPR.

### 6.2) I diritti non subordinati a una richiesta dell'interessato

Pur in assenza di richiesta da parte dell'interessato, il Titolare garantisce che allo stesso sia fornita idonea informativa al momento della raccolta dei suoi Dati personali presso lo stesso o, se i Dati non sono raccolti direttamente presso l'interessato, entro i seguenti termini:

- entro un termine ragionevole dall'ottenimento dei Dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i Dati personali sono trattati;
- nel caso in cui i Dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei Dati personali.

## 7) Misure di sicurezza (Art. 32 GDPR)

Il Titolare adotta le misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Tali misure devono essere altresì idonee a prevenire ogni violazione di Dati personali, ivi incluse la distruzione, perdita, modifica, divulgazione o l'accesso non autorizzato a Dati personali, effettuati in modo accidentale o illegale. Qualora si verifichi una violazione di Dati personali, le misure tecniche e organizzative adottate devono comunque essere in grado di riconoscere e contrastare l'avvenuta violazione.

## 8) La valutazione d'impatto sulla protezione dei dati personali – DPIA (Art. 32 GDPR)

Nel caso in cui un determinato tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche (ad esempio perché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento), è necessario effettuare una valutazione dell'impatto prima di procedere al trattamento stesso.
Ogni qualvolta sia previsto un nuovo trattamento, sia modificato un trattamento esistente o comunque muti il rischio presentato da un trattamento svolto, il Titolare consulta il DPO (ove nominato), valuta la necessità o opportunità di effettuare una valutazione di impatto sulla protezione dei Dati personali in considerazione del rischio presentato dal trattamento e applicando la metodologia di analisi d'impatto sul trattamento dei dati personali basata sul PDCA (Plan, Do, Check, ACT).
Qualora la valutazione di impatto sulla protezione dei Dati personali evidenzi un rischio elevato per gli interessati, con il supporto del DPO (ove nominato), deve essere valutata l'adozione di ulteriori misure per attenuare il rischio e/o la necessità di effettuare una consultazione preventiva con il Garante. Eventuali successivi suggerimenti del Garante sono immediatamente recepiti prima di procedere al trattamento oggetto della DPIA.
Per i trattamenti già sottoposti a DPIA è prevista una revisione di tali valutazioni almeno ogni 2 anni.

## 9) Data breach (Artt. 33 e 34 GDPR)

Qualora si verifichi una violazione di Dati personali, le misure tecniche e organizzative adottate devono comunque essere in grado di riconoscere e contrastare l'avvenuta violazione.
Nel caso in cui si verifichi una violazione dei Dati personali che presenti un rischio per le libertà e i diritti degli interessati, il Titolare prevede una modalità immediata di reazione che permetta:

- la notifica dell'avvenuta violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza e, se ricorrono i presupposti, all'interessato;
- l'adozione delle misure necessarie ad attenuare gli effetti negativi della violazione.
- Il Titolare tiene un registro delle violazioni e stabilisce procedure interne che disciplinano il suo aggiornamento al sussistere di ogni violazione, indifferentemente dal rischio presentato per i diritti e le libertà degli interessati e meccanismi di conservazione di tutte le comunicazioni riguardanti la violazione. In registro sono indicati tutti gli elementi richiesti dalla normativa applicabile, tra cui:
- le circostanze relative alla violazione;
- le conseguenze;
- le misure adottate per contrastarla e limitarne gli effetti;
- i Dati personali coinvolti; informazioni adeguate per permettere al Titolare di determinare le motivazioni per non aver effettuato la notifica, o averla effettuata in ritardo.

Il processo di gestione del Data Breach è dettagliato nella relativa Procedura (Data Breach Policy)

## 10) Il sistema delle relazioni e dei flussi informativi

Sono definiti flussi informativi volti ad assicurare al Titolare, agli incaricati della Società, la piena conoscenza e governabilità degli adempimenti in materia di protezione dei Dati personali.
Il sistema delle relazioni deve essere costituito sia da flussi informativi codificati derivanti da attività con periodicità definita e/o tempistica certa, sia da informative prodotte all'occorrenza che possono essere predisposte anche in maniera non strutturata.

In particolare, sono garantiti almeno i seguenti flussi informativi:

- reporting verso il Titolare, qualora siano riscontrate irregolarità o problematiche di particolare gravità deve essere fornita una pronta informazione anche al Titolare del trattamento;
- reporting costante al Titolare del trattamento da un Referente privacy che rendiconta, almeno annualmente, i principali accadimenti in materia di protezione dei Dati personali relativi ai trattamenti di propria competenza;
- reporting costante al Titolare del trattamento e da Referente privacy in merito ad ogni problematica riscontrata inerente il trattamento dei Dati personali.

## 11) Allegati

La presente Policy è integrata dai documenti di seguito allegati:

- Allegato 1: Compiti del DPO
- Allegato 2: Compiti del Referente privacy (se nominato)

**Policy in materia di protezione dei dati personali - Allegato 1**
**COMPITI DEL DPO**

Il DPO e la struttura organizzativa a suo supporto rappresentano la principale funzione di consultazione, consulenza, sorveglianza e controllo in materia di protezione dei dati personali.

In conformità al Regolamento, il DPO se nominato[1] è incaricato almeno dei seguenti compiti:

- verificare nel continuo il rispetto della normativa interna ed esterna in materia di protezione dei dati personali da parte delle unità organizzative del Titolare, mediante richiesta di documenti e/o accesso a tutte le banche dati contenenti informazioni utili all'espletamento dei propri compiti;
- informare e fornire consulenza al Titolare, nonché ai relativi incaricati del trattamento in merito agli obblighi derivanti dal Regolamento nonché dall'ulteriore normativa in materia di protezione dei dati personali;
- fornire supporto e pareri al Titolare del trattamento ed agli incaricati del trattamento in merito all'interpretazione della normativa interna ed esterna in materia di protezione dei dati personali e alle corrette modalità di trattamento dei dati personali;
- sorvegliare l'osservanza del Regolamento e dell'ulteriore normativa interna o esterna in materia di protezione dei dati personali nonché delle politiche del Titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- collaborare con il Titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
- cooperare con il Garante;
- monitorare l'evoluzione della normativa e informare il Titolare in merito alla necessità di aggiornamenti della documentazione privacy e della normativa interna che si rendano necessari alla luce di tali evoluzioni normative;
- raccogliere dalle singole unità organizzative competenti le segnalazioni in merito alla necessità di aggiornamento della normativa interna;
- proporre al Consiglio di Amministrazione l'aggiornamento della normativa interna in materia di protezione dei dati personali alla luce del complessivo livello di conformità alla normativa tempo per tempo applicabile in materia;
- coordinare e gestire i flussi informativi in ambito privacy all'interno della struttura organizzativa del Titolare;
- fungere da punto di contatto con gli interessati e il Garante per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
- tenendo conto della natura del trattamento, assistere il titolare del trattamento con misure tecniche e organizzative adeguate, al fine di riscontrare le richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR 2016/679.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

[1] Se non nominato i compiti elencati potranno essere svolti dal Titolare

**Policy in materia di protezione dei dati personali - Allegato 2**
**COMPITI DEL REFERENTE PRIVACY**

Al Referente Privacy, se nominato[2], sono attribuite almeno le seguenti mansioni:

**In particolari, il Referente interno Privacy è tenuto a:**

- Osservare il GDPR 2016/679 e il D.Lgs. 30 giugno 2003, n. 196, il D.Lgs. 101/2018 e le altre disposizioni legislative e regolamentari in materia di *data protection*;
- Trattare i dati delle persone nel rispetto dei principi di liceità e correttezza;
- Attenersi alle istruzioni del Titolare;
- Curare l'implementazione, la diffusione e l'aggiornamento del Sistema di Gestione Privacy della Società ;
- Collaborare ed interagire con il DPO nominato per l'attuazione delle prescrizioni impartite dall'Autorità Garante per la Protezione dei dati personali;
- Interagire con i Clienti titolari del trattamento, i soggetti incaricati di eventuali verifiche, controlli o ispezioni.
- Supportare gli incaricati della Società .
- Decidere, in accordo con il Titolare del trattamento dei dati, con il coinvolgimento del DPO, se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura titolare avvalendosi della consultazione della policy delle linee guida fornitori ;
- Individuare i soggetti da nominare quali Responsabili secondo requisiti di esperienza, capacità, affidabilità e sicurezza;
- Assistere il Titolare, con il supporto del DPO, nella nomina ed incarico per iscritto di uno o più incaricati della gestione e della manutenzione degli strumenti elettronici, degli Amministratori di Sistema e della loro valutazione periodica, dell'incaricato della custodia delle copie delle credenziali e dell'incaricato delle copie di sicurezza delle banche dati, se il trattamento è effettuato con mezzi informatici. Inoltre, dovrà definire, in accordo con il personale tecnico della Società , delle procedure tecnico-organizzative e documentali che:
  - Consentano di ripristinare tempestivamente, e opportunamente documentare, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - Consentano di testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento.
- Far sì che chiunque agisca sotto l' autorità del Titolare della Società , e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o la normativa nazionale vigente. Quindi, pianificare corsi di formazione ed informazione con il contributo del DPO.

**Disposizioni generali in materia di trattamento dei dati**

- esaminare gli aggiornamenti della normativa segnalati dal DPO e divulgarli all'interno della Società ;
- ricevere qualsiasi richiesta di consulenza da parte degli incaricati e del Titolare e, a seconda della complessità del quesito, (i) trasmetterla immediatamente al DPO, o (ii) rispondere direttamente;
- coadiuvare le funzioni competenti nella gestione dei diritti degli interessati qualora una richiesta presenti alcune problematiche e/o difficoltà che non richiedono l'intervento del DPO;
- sovrintendere il processo di selezione e nomina dei responsabili esterni e informare il DPO sullo svolgimento della procedura;
- organizzare corsi di formazione in ambito privacy in linea con il piano approvato dal DPO;
- curare l'implementazione della documentazione e della normativa interna in materia di privacy;
- partecipare attivamente allo svolgimento delle analisi di privacy by design assicurando il rispetto della metodologia predisposta dal DPO, aggiornare costantemente il DPO e coinvolgerlo qualora risulti necessario;
- effettuare verifiche periodiche con report documentati presso i Responsabili esterni del Titolare, eventualmente avvalendosi delle risultanze di Questionari di verifica ed informare il DPO sugli esiti delle verifiche. Nel caso in cui il processo di verifica evidenzi una criticità, ivi inclusa una qualsiasi forma di inadempimento da parte del fornitore, coinvolgere immediatamente il DPO;
- gestire e aggiornare l'elenco dei responsabili esterni, assicurando che siano sempre indicati tutti i Responsabili esterni nominati;

[2] Se non nominato i compiti elencati potranno essere svolti dal DPO nominato o dal Titolare.

- gestire e aggiornare l'elenco dei responsabili interni / amministratori, assicurando che siano sempre indicati tutti i soggetti nominati;
- ricevere ed eseguire ogni comunicazione del DPO, ivi inclusa la trasmissione delle istruzioni del DPO alle funzioni coinvolte;
- ricevere ogni segnalazione da parte del personale del Titolare su problematiche e criticità riscontrate in materia di protezione dei dati personali e informare prontamente il DPO;
- partecipare ad incontri periodici con il DPO;
- ricevere ogni segnalazione relativa alla violazione di dati personali relativa al Titolare e informare prontamente il DPO indicando, ove conosciuta, l'origine della violazione;
- coinvolgere il DPO qualora la gestione di una richiesta da parte di un interessato presenti particolari problematiche e/o l'interessato abbia richiesto il diretto intervento del DPO;
- trasmettere al DPO qualsiasi comunicazione o richiesta del Garante, e informarlo sull'eventuale volontà del Titolare e/o di una delle funzioni della Società di contattare il Garante per qualsivoglia motivo;
- redigere un report annuale indirizzato al DPO e al Consiglio di Amministrazione del Titolare riguardante le attività svolte;
- assicurare che tutto il personale che tratta dati personali sia stato appositamente nominato incaricato del trattamento.
- se il trattamento è effettuato con mezzi informatici, dovrà far redigere, aggiornare, e verificare ad ogni variazione, l'elenco dei sistemi di elaborazione, con l'Amministratore di Sistema;
- definire e successivamente verificare, con cadenza almeno semestrale, le modalità d'accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia;
- comunicare tempestivamente al Titolare gli eventuali nuovi trattamenti che si rende necessario intraprendere, curando gli adempimenti necessari per assicurarne la legittimità e la sicurezza;
- attuare gli obblighi di informativa e di acquisizione del consenso nei confronti degli interessati;
- aggiornare e/o distruggere i dati personali detenuti tenuto conto degli obblighi legali di conservazione;

**Verifiche periodiche**

- Verificare ed eventualmente aggiornare almeno annualmente tutte le informazioni contenute nel registro delle attività di trattamento, come previsto dall'art. 30 c. 2 GDPR 2016/679;
- Qualora il trattamento dei dati sia affidato, in tutto o in parte, all'esterno della struttura del titolare, supportare il DPO nelle attività di controllo, annuale, affinchè le misure di sicurezza riguardanti i dati personali siano applicate dai Responsabili esterni del trattamento, con l'invio di Questionari di verifica e se del caso anche mediante visite ispettive;
- Supportare il DPO nelle attività di verifica, con cadenza almeno trimestralmente, il grado di compliance dell'organizzazione della Società rispetto alla vigente normativa in materia di dati personali, nonché il buon funzionamento, la corretta applicazione e la conformità alle prescrizioni del Garante Privacy dei sistemi e delle misure di sicurezza adottate;
- Contribuire, a seguito di ciascuna verifica, alla stesura della relazione scritta dal DPO, anche in formato elettronico, da trasmettersi al Titolare del trattamento;
- Supportare il DPO nel monitoraggio costante dell'adeguatezza delle misure di sicurezza adottate.

**Misure tecnico-organizzative di sicurezza**

- Supportare il DPO al fine di adottare ed aggiornare misure tecnico-organizzative idonee a garantire la sicurezza dei trattamenti di dati personali e in linea con le prescrizioni di cui all'art. 32 GDPR 2016/679 ed ogni altra disposizione in materia di tutela dei dati personali.
- Supportare il DPO nell'adozione e nel rispetto delle misure di sicurezza individuate e richieste dal Titolare del Trattamento;
- Supportare il DPO nel garantire la corretta applicazione di tutte le misure di sicurezza adottate, assicurando su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

**Valutazioni d'impatto e del rischio**

- Supportare il DPO nello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio, qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'esito della valutazione dev'essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta la normativa vigente.

- Supportare il DPO nel valutare e documentare l'adeguato livello di sicurezza, dei rischi presentati dal trattamento, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

**Gestione eventi dannosi (Data breach)**

Nel caso si verifichi un evento dannoso (data breach), comunicare tempestivamente al Titolare del trattamento ed al DPO, l'accaduto e contribuire alla valutazione della necessità di notifica all'Autorità preposta (Data Breach ex artt. 33 e 34 GDPR 2016/679), qualora si registri una violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Inoltre, dovrà tenere aggiornato, su indicazioni del DPO, aggiornando il Titolare, l'apposito registro interno dei Data Breach, ove riporterà i dati essenziali relativi all'evento e le valutazioni ed azioni conseguenti.

Non è consentito al referente interno comunicare a terzi i dati personali trattati, salvo che la comunicazione sia indispensabile per lo svolgimento delle sue attività e avvenga nei confronti di terzi autorizzati dal Titolare, oppure avvenga nei confronti di organi giurisdizionali, o avvenga nell'adempimento di norme di legge, di regolamenti, di provvedimenti delle autorità, fatta salva in ogni caso diversa istruzione del Titolare.

ALLEGATO B

**Policy per la tutela ambientale**

## 1 SCOPO E RIFERIMENTI

La presente policy ha lo scopo di disciplinare i principi comportamentali e le linee guida alle quali la Società OFF. MECCANICA DI MARA GIANMARIO & C. S.R.L. e tutto il personale devono osservare per la gestione degli adempimenti in campo ambientale al fine di garantire la conformità alla normativa di riferimento e prevenire la commissione di reati di tipo ambientale.
I riferimenti principali sono i seguenti

- Decreto Legislativo 231/2001 e ss.mm.ii (di seguito anche D.lgs. 231/2001);
- "Codice Etico" di Officine Mara
- "Modello di Gestione, Organizzazione e Controllo" di Officine Mara ai sensi e per gli effetti di cui al D. Lgs. 231/2001.

## 2 MODALITÀ DI GESTIONE DELLE ATTIVITA'

E' fatta premessa che Officine Mara, inserita nel territorio con storia decennale, è attenta al rispetto dell'ambiente circostante.
In particolare, l'Azienda opera nel rispetto dell'ambiente (comprendendosi in detto termine l'aria, l'acqua, il suolo, il sottosuolo, un ecosistema, le risorse naturali, la flora, la fauna, gli esseri umani e le loro interrelazioni), in conformità con le disposizioni normative vigenti in materia e nel rispetto del Codice Etico.

Officine Mara rispetta e pretende il rispetto – sia a livello interno all'azienda sia a livello esterno – della normativa ambientale prevenendo e contrastando tutti i comportamenti atti ad offendere o, anche solo, a mettere in pericolo la salvaguardia dell'ambiente, in tutte le sue espressioni.
E' fatto divieto di qualunque condotta, dolosa o colposa, che possa mettere in pericolo o ledere l'ambiente, inteso in tutte le sue espressioni (flora, fauna, acqua, aria, suolo etc.), con particolare – ma non esclusivo – riferimento alle aree naturali protette o sottoposte a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ed alle specie animali o vegetali protette.
Pertanto, l'Azienda, nell'espletamento delle proprie attività, previene ed impedisce qualunque forma di inquinamento, sia esso dell'acqua, del suolo, del sottosuolo, di un ecosistema, dell'aria, elettromagnetico, acustico etc..

L'Azienda e tutti i collaboratori e destinatari sono tenuti al tracciamento di ogni attività in ambito ambientale, con particolare riferimento alla documentazione prevista *ex lege* ed ad ogni attività di impatto con la normativa ambientale.

L'ODV ha facoltà di accesso a tale documentazione e facoltà di nomina di un consulente esterno in ambito ambientale per l'approfondimento delle tematiche.

**Gestione dei rifiuti**
Officine Mara e tutti i destinatari devono:

- ✓ ottemperare alle normative in materia di gestione dei rifiuti,
- ✓ astenersi dal deposito incontrollato dei rifiuti e dall'abbandono degli stessi.

All'atto del conferimento di rifiuti, Officine Mara deve verificare il possesso degli idonei atti autorizzatori del destinatario del rifiuto e del trasportatore.

**Rimozione, recupero, smaltimento rifiuti e ripristino dello stato dei luoghi in caso di avvenuto abbandono dei rifiuti stessi, nonché all'eventuale bonifica**

- ✓ nel caso in cui si sia verificato l'abbandono dei rifiuti, Officine Mara è tenuta ad informare immediatamente l'ODV ed a rimuovere, recuperare e smaltire immediatamente i rifiuti stessi, provvedendo al ripristino dello stato dei luoghi;

- ✓ qualora l'abbandono dei rifiuti sia accertato dal Comune ove esso è avvenuto e, di conseguenza, il Sindaco disponga con ordinanza le operazioni necessari per i fini di cui al punto precedente, l'Azienda è tenuta ad informare immediatamente l'ODV ed a porre in essere senza indugio le misure disposte dall'ordinanza comunale;
- ✓ l'ODV vigila sulla tempestiva ottemperanza all'Ordinanza Comunale;
- ✓ in caso di inquinamento, deve provvedere alla comunicazione dell'evento agli Enti di controllo nei tempi previsti dalla normativa, alla esecuzione degli interventi di messa in sicurezza di emergenza possibili in relazione all'evento e alla presentazione degli studi e progetti indicati dal d.lgs. 152/06 - Titolo V Parte IV- ed alla successiva bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui all'art. 242 ss. d.lgs. 152/2006;
- ✓ delle attività di cui ai punti che precedono l'Azienda dà adeguata traccia, costituendo apposito archivio di tutti gli atti inerenti a suddette attività.

**Emissioni**

- ✓ nell'esercizio delle attività, Off Mara garantisce di mantenere in validità l'idonea autorizzazione; la scadenza, la decadenza, la sospensione o la revoca dell'autorizzazione comportano l'immediata sospensione delle attività sino alla nuova vigenza dell'autorizzazione;
- ✓ l'Azienda esercita l'attività nel rispetto dei limiti autorizzati; i controlli prescritti dalle autorizzazioni vengono eseguiti secondo le periodicità stabilite a livello autorizzatorio e legale;
- ✓ in presenza di eventi anomali, l'Azienda attua le azioni prescritte dall'atto autorizzatorio;
- ✓ l'Azienda costituisce apposito archivio contenente le autorizzazioni alle emissioni e le analisi svolte; tale fascicolo è a disposizione dell'ODV.

I destinatari tutti sono tenuti a segnalare all'ODV ogni evento afferente alla tematica della gestione ambientale che possa far presumere una violazione dei protocolli ambientali, nonché ogni comunicazione proveniente dalla P.A.
A titolo esemplificativo e non esaustivo, devono essere trasmessi all'ODV:

- eventuali verbali o prescrizioni rilasciati dalle Pubbliche Autorità in materia ambientale, a prescindere dal loro esito;
- eventuali verbali interni ispettivi che abbiano dato esito positivo ovvero eventuali audit che abbiano rivelato anomalie o criticità in ambito ambientale;
- eventuali verbali dell'ente certificatore;
- eventuali comunicazioni sui provvedimenti disciplinari adottati nei confronti dei dipendenti che abbiano posto in essere comportamenti non conformi alle disposizioni normative ed aziendali in materia di tutela dell'ambiente.

Tutta la documentazione in ambito ambientale non rientrante tra quella di cui sopra, deve essere esibita all'ODV a semplice richiesta.

Copia di tutta la documentazione sopra indicata relativa alle singole fasi del processo deve essere disponibile per eventuali verifiche da parte dell'OdV.

## 4 EFFICACIA VINCOLANTE DELLA POLICY

Il mancato rispetto di quanto stabilito nella presente policy può comportare l'applicazione di sanzioni disciplinari al personale dipendente di OFFICINE MARA fino alla chiusura unilaterale del rapporto di lavoro.
Il documento costituisce parte integrante del Modello della Società.
L'inosservanza dei principi e delle regole ivi contenuti rappresenta una violazione del Modello e comporta l'applicazione del sistema disciplinare adottato ai sensi del Modello stesso.

Tutte le Funzioni aziendali coinvolte nelle attività di cui alla presente policy hanno la responsabilità di osservare e far osservare il contenuto.
Devono altresì segnalare tempestivamente all'Organismo di Vigilanza ogni evento suscettibile di incidere sull'operatività e sull'efficacia della policy stessa.
La comunicazione all'Organismo di Vigilanza delle eventuali segnalazioni avviene tramite posta elettronica alla seguente casella di posta odv.@officinemara.it/manuela.belletti@methaconsulting.it