# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

# (INFORMATION SECURITY)

*Data pubblicazione 4/12/2025*

*Versione n°2*

Sommario

## 1. PREMESSA

La sicurezza delle Informazioni è un elemento strategico per METLAC Group, in quanto garantisce la protezione del patrimonio informativo, la resilienza operativa e la conformità normativa. In un contesto di crescente digitalizzazione e minacce cyber, METLAC Group ha adottato un Sistema di Gestione Integrato che adotta lo schema di Sicurezza Informatica **Information Security Management System (ISMS)** conforme alla Direttiva NIS2 e ispirato alle migliori pratiche internazionali, come la norma ISO/IEC 27001, il cybersecurity framework del NIST e le linee guida ENISA e del Disaster Recovery Institute (DRI International).

La presente Politica per la Sicurezza delle Informazioni rappresenta una derivazione e approfondimento specifico della POLITICA AZIENDALE e si integra con le politiche esistenti in materia di Continuità Operativa, Trattamento Dati e Regolamento ICT, e si basa sulla guida ENISA "Cybersecurity Roles and Skills for NIS2 Essential and Important Entities" (Giugno 2025).

Inoltre la presente costituisce la revisione 2 della precedente "POLITICA TRATTAMENTO DATI E INFORMAZIONI SENSIBILI" pubblicata in data 09/12/2024, con estensione del campo di applicazione alla Sicurezza delle Informazioni, ben oltre il precedente quadro relativo alla Privacy e in particolare in attuazione al Regolamento GDPR; METLAC Spa quale capofila delle società di METLAC Group, ai sensi dell'art.13 del GDPR provvede a informare i portatori di interessi in merito ai dati personali e le informazioni sensibili che saranno trattate esclusivamente al fine dell'instaurazione, del perfezionamento e della gestione del rapporto di business di interesse, secondo i principi di correttezza, liceità e trasparenza, tutelando la riservatezza e nel rispetto della normativa richiamata. In particolare, METLAC Group si impegna a rispettare la *privacy* di clienti, fornitori, dipendenti, candidati, Soci e Cariche Sociali e di tutti i soggetti con cui intrattiene rapporti commerciali, garantendo elevati standard di protezione nel trattamento dei dati personali, siano essi relativi al personale interno o agli utenti esterni.

## 2. AMBITO DI APPLICAZIONE

La presente politica definisce i principi, le responsabilità e le misure per garantire la sicurezza delle informazioni e dei sistemi digitali. Si applica a tutte le informazioni, di natura personale e non, raccolte, conservate, utilizzate o altrimenti trattate da METLAC Group, in qualsiasi formato, inclusi documenti informatizzati, informazioni di tipo elettronico e documenti cartacei. I termini della presente Politica valgono anche per agenti e appaltatori che gestiscono e trattano informazioni personali per conto di METLAC Group. La presente Politica si applica e viene distribuita indistintamente a tutti i livelli aziendali:

- Dipendenti, organi direttivi e amministrativi
- Collaboratori, fornitori, partner, outsourcer

Il campo di applicazione riguarda inoltre:

- i dati trattati, inclusi quelli personali, particolari e giudiziari

- le informazioni aziendali, quali asset intangibili
- i dispositivi aziendali e le infrastrutture di informazione e telecomunicazioni (ICT)
- il sistema informativo interno, gli ERP, i servizi informatici e i processi digitali (IT)
- i sistemi hardware e software che gestiscono e controllano i processi industriali (OT).

## 3. PRINCIPI

I principi a cui si ispira METLAC Group per garantire la Sicurezza Informatica sono:

- **Riservatezza**: tutela delle informazioni contro accessi non autorizzati
- **Integrità**: garanzia della completezza e dell'inalterabilità dei dati
- **Disponibilità**: assicurazione di un accesso costante e affidabile alle informazioni
- **Responsabilità**: possibilità di tracciamento e attribuzione delle azioni svolte
- **Conformità**: aderenza ai requisiti normativi e alle policy aziendali

## 4. RIFERIMENTI NORMATIVI

- Regolamento UE 2016/679 (General Data Protection Regulation – GDPR);
- D.lgs. 196/2003 (Codice della Privacy), che regolamenta il trattamento dei dati personali e implementa le normative europee;
- D.lgs. 101/2018, che adegua il Codice della Privacy italiano al Regolamento UE 2016/679;
- Direttiva (UE) 2022/2555 (NIS2)
- ISO/IEC 27001:2022 – Information Security Management System
- ISO/IEC 27005:2022 – Guidance on management Information Security Risks
- ISO/IEC 27035 – Information Security Incident Management
- ISO/IEC 22301:2019 – Business Continuity Management
- ISO/IEC 31000:2018 – Risk Management Guidelines

## 5. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Per garantire la protezione del patrimonio informativo, la continuità operativa e la conformità normativa, METLAC Group adotta un insieme strutturato di misure tecniche e organizzative, conforme ai requisiti della Direttiva NIS2 e ispirata alla norma ISO/IEC 27001 e alle migliori pratiche di settore.

### a. Gestione degli accessi e autenticazione

- Tutti gli utenti METLAC accedono ai sistemi aziendali tramite credenziali personali, gestite centralmente tramite Active Directory.
- L'autenticazione a due fattori (2FA) è obbligatoria per l'accesso a sistemi critici, piattaforme cloud (Microsoft 365, OneDrive, Teams) e VPN.
- I privilegi di accesso sono assegnati secondo il principio del minimo privilegio e rivisti almeno ogni sei mesi dal reparto IT.
- Gli accessi privilegiati ai sistemi sensibili sono strettamente controllati, monitorati e gestiti attraverso soluzioni di Privileged Access Management (PAM), con revoche tempestive e riesami periodici basati sulla necessità operativa.
- L'accesso remoto è consentito solo tramite VPN aziendale sicura, con autenticazione forte e monitoraggio degli accessi.

### b. Protezione delle postazioni di lavoro e dispositivi mobili

- Tutti i PC e notebook aziendali sono dotati di antivirus centralizzato, firewall personale e cifratura dei dati tramite BitLocker.
- I dispositivi mobili (smartphone, tablet) e le SIM aziendali sono gestiti tramite Mobile Device Management (MDM), con policy di blocco remoto, cancellazione dati e aggiornamento automatico.
- È vietato l'utilizzo di dispositivi personali per attività lavorative senza preventiva autorizzazione e verifica di conformità alle policy di sicurezza METLAC.

### c. Sicurezza della rete e delle infrastrutture

- La rete aziendale METLAC è segmentata per isolare i sistemi critici e limitare la propagazione di eventuali attacchi.
- Sono implementati firewall di nuova generazione, sistemi IDS/IPS e monitoraggio continuo del traffico di rete.
- Tutti gli accessi Wi-Fi aziendali sono protetti da autenticazione WPA2/WPA3 e segregati rispetto alle reti guest.
- Il traffico di rete è soggetto a logging centralizzato e alert automatici per rilevare comportamenti anomali.

### d. Gestione delle vulnerabilità e aggiornamenti

- Il patch management è centralizzato: tutti i sistemi e le applicazioni sono aggiornati automaticamente secondo un piano mensile e in caso di vulnerabilità critiche.
- Sono previsti vulnerability assessment trimestrali e penetration test annuali sulle infrastrutture e sulle applicazioni critiche.

- Le vulnerabilità rilevate sono classificate per gravità e gestite secondo procedure di remediation con tempi definiti (SLA).

### e. Protezione dei dati e backup

- I dati aziendali sono archiviati su server sicuri e su cloud Microsoft 365, con backup automatici giornalieri e test di ripristino trimestrali.
- È vietato il salvataggio di dati aziendali su dispositivi personali o cloud non autorizzati.
- I backup sono cifrati e conservati in siti separati per garantire data recovery e business continuity in ottica di resilienza operativa.

### f. Sicurezza delle applicazioni e dei servizi cloud

- L'utilizzo di servizi cloud è consentito solo su piattaforme approvate, rese disponibili entro il territorio della UE, e conformi alle linee guida di ACN e allo standard ISO/IEC 27017.
- Le applicazioni sviluppate internamente sono sottoposte a code review, test di sicurezza e validazione prima della messa in produzione.
- È vietato l'uso di cloud pubblici non autorizzati per la gestione di dati aziendali.

### g. Gestione della sicurezza dei fornitori e della supply chain

- I fornitori critici sono valutati e selezionati anche in base ai requisiti di sicurezza delle informazioni, con audit periodici e verifica delle certificazioni.
- I contratti prevedono clausole specifiche su protezione delle informazioni, gestione degli incidenti, accordi di confidenzialità, affidabilità e resilienza e diritto di audit da parte di METLAC.
- È previsto un monitoraggio periodico della sicurezza dei fornitori e delle terze parti che trattano dati o servizi critici.

### h. Protezione della posta elettronica e della navigazione

- Tutte le caselle e-mail aziendali sono protette da sistemi antispam, antiphishing e sandboxing degli allegati.
- La navigazione internet è filtrata e monitorata tramite proxy e firewall per prevenire accessi a siti malevoli o non conformi alle policy METLAC.
- Sono previste campagne periodiche di sensibilizzazione contro le minacce di phishing e social engineering.

### i. Monitoraggio, logging e audit

- Tutti gli accessi, le operazioni critiche e gli eventi di sicurezza sono registrati in log centralizzati, conservati secondo policy definite e soggetti a revisione periodica.
- Il Security Operations Center as a Service (SOCaaS) monitora costantemente gli eventi di sicurezza e attiva le procedure di risposta in caso di anomalie.
- Sono previsti audit interni ed esterni annuali per verificare l'efficacia delle misure adottate e la conformità agli standard e alle policy METLAC.

Tutte le misure sono soggette a revisione periodica e aggiornamento in funzione dell'evoluzione delle minacce, delle tecnologie e delle normative di riferimento. Le procedure operative dettagliate sono disponibili sul portale SQHSE.

j. Segregazione di Ruoli e Responsabilità

- Le responsabilità relative alla sicurezza sono chiaramente definite e assegnate, garantendo che nessun singolo individuo abbia il controllo completo su un processo critico e i ruoli siano segregati su diversi livelli di governo e controllo (principio della segregazione dei compiti, o Segregation of Duties - SoD).
- È stabilita una chiara catena di responsabilità che definisce i proprietari dei rischi, i responsabili degli asset informativi e coloro che sono incaricati dell'implementazione delle misure di controllo.

Tutte le definizioni di ruolo e le matrici di responsabilità sono formalizzate nei documenti organizzativi ufficiali e sono sottoposte a revisione almeno annuale da parte della Direzione per adattarsi ai cambiamenti della struttura aziendale e dei requisiti normativi. La conformità ai principi di SoD è verificata come parte degli audit interni.

k. Formazione e consapevolezza

- Viene erogato un programma di formazione annuale obbligatorio sulla sicurezza delle informazioni e sulla protezione dei dati per tutti i dipendenti, i collaboratori e il personale esterno con accesso ai sistemi aziendali. Questo include moduli specifici su *phishing*, ingegneria sociale, gestione delle password e procedure di *incident response*.
- Si effettuano regolarmente campagne di *phishing* simulate e altre attività di test per valutare il livello di consapevolezza del personale e identificare aree che necessitano di ulteriore formazione mirata. I risultati vengono utilizzati per migliorare il contenuto dei corsi.
- La consapevolezza sui rischi e sulle policy di sicurezza è mantenuta alta attraverso comunicazioni periodiche su nuove minacce, vulnerabilità e aggiornamenti delle policy aziendali.

L'efficacia della formazione è misurata attraverso test di valutazione e l'analisi del tasso di successo nelle simulazioni di attacco. Il materiale didattico e il programma formativo sono aggiornati semestralmente in collaborazione con le funzioni aziendali preposte, così da riflettere l'evoluzione delle minacce e le modifiche legislative.

## 6. GESTIONE DEGLI INCIDENTI E DELLE CRISI

METLAC Group adotta un processo strutturato per la gestione degli incidenti di sicurezza delle informazioni, conforme alla Direttiva NIS2 e allo standard ISO 22301. Tale processo è ispirato alla ISO/IEC 27001 e ISO 27035, al framework NIST e alle best practice DRI e ENISA. L'obiettivo è garantire una risposta tempestiva, efficace e tracciabile a qualsiasi evento che possa compromettere la riservatezza, l'integrità o la disponibilità delle informazioni e dei sistemi aziendali.

1. Definizione di incidente

Per incidente di sicurezza si intende qualsiasi evento, intenzionale o accidentale, che abbia un impatto negativo sulla sicurezza delle informazioni, dei sistemi digitali o dei servizi aziendali (es. malware, phishing, perdita dati, accesso non autorizzato, interruzione di servizio).

## 2. Fasi del processo di gestione incidenti

### a) Rilevazione e segnalazione

- Tutti i dipendenti, collaboratori e fornitori sono tenuti a segnalare tempestivamente qualsiasi sospetto incidente o anomalia al first contact (incident responder) tramite i canali ufficiali (helpdesk, e-mail dedicata, portale QHSE&S).
- Il Security Operations Center as a Service (SOCaaS) monitora costantemente i sistemi e genera alert automatici in caso di eventi sospetti.

### b) Classificazione e valutazione

- Gli incidenti vengono classificati in base a gravità, impatto e urgenza: minor, major, hot e critical.
- Il CISO, in collaborazione con il Cyber Incident Responder, valuta la natura dell'incidente e attiva il piano di risposta (IRP).

### c) Contenimento, mitigazione ed eradicazione

- Vengono adottate misure immediate per contenere e mitigare l'incidente, eradicandone la causa e limitandone la propagazione (es. isolamento di sistemi compromessi, blocco account, disconnessione dalla rete).
- Si attivano le procedure di backup e ripristino se necessario.

### d) Analisi forense e investigazione

- Se necessario, il Digital Forensics Expert raccoglie e analizza le evidenze digitali per ricostruire la dinamica dell'incidente, identificare la causa e valutare l'impatto, garantendo la sicurezza della catena di custodia.
- Tutte le attività sono documentate in un registro incidenti dedicato.

### e) Comunicazione interna ed esterna

- Il CISO informa tempestivamente il management e, se necessario, il Consiglio di amministrazione.
- In caso di incidenti significativi ad impatto "hot" o "critical", viene attivata la comunicazione preliminare verso il CSIRT nazionale entro 24 ore dall'evento, come previsto dalla NIS2, a cui saranno forniti ulteriori dettaglio entro 72 ore dall'evento e conclusive entro 1 mese dall'evento.
- Se l'incidente coinvolge dati personali, viene valutata la necessità di notifica all'Autorità Garante e agli interessati, entro 72 ore dall'evento.

### f) Recupero e ripristino

- Se necessario, si attiva il piano di Business Continuity e l'attivazione delle procedure di Disaster Recovery, così da ripristinare i sistemi e presso i siti secondari individuati all'interno delle strategie di continuità operativa.
- Viene verificata la completa rimozione delle minacce e il ritorno alla piena operatività.

**g) Revisione post-incidente, apprendimento e miglioramento continuo**

- Dopo la chiusura dell'incidente, viene effettuata una revisione ("post-mortem") per identificare le cause profonde, le aree di miglioramento e aggiornare le procedure e i rischi.
- Le lezioni apprese vengono condivise con le parti interessate e il personale viene aggiornato attraverso sessioni di formazione e aggiornamento.

**3. Ruoli e responsabilità**

- **CISO**: Coordinamento generale, attivazione del piano IRP, comunicazione con il management e le autorità.
- **Cyber Incident Responder e Incident Response Structure**: Gestione operativa dell'incidente e della crisi.
- **Digital Forensics Expert**: Raccolta e analisi delle evidenze digitali.
- **SOCaaS**: Monitoraggio, rilevazione e primo alert.
- **Tutti i dipendenti**: Segnalazione tempestiva di incidenti o anomalie.

**4. Registro incidenti e audit**

- Tutti gli incidenti sono registrati in un apposito registro, con dettagli su data, natura, impatto, azioni intraprese e stato di risoluzione.
- Il registro è soggetto a revisione periodica da parte dell'ISMS Auditor e del management.

**5. Test e simulazioni**

- METLAC Group organizza periodicamente simulazioni di incidenti (table-top exercise, phishing simulation, test di Business Continuity) per verificare l'efficacia delle procedure e la prontezza del personale.

## 7. TRATTAMENTO DEI DATI

Il Titolare del Trattamento è METLAC SPA, con sede legale in S.S. 35 Bis dei Giovi, 53, CAP 15062, Bosco Marengo (AL), Italia e, secondo i casi, le sue Società controllate.

Il trattamento dei dati personali in METLAC Group avviene nel pieno rispetto dei diritti e della riservatezza degli interessati. I dati sono trattati in modo lecito, trasparente e confidenziale e sono adottati i seguenti principi:

- **Finalità e limitazione**: I dati personali vengono raccolti e trattati esclusivamente per scopi specifici e legittimi, che devono essere chiaramente definiti prima della raccolta. Modifiche successive agli scopi originali sono ammesse solo se strettamente correlate agli scopi iniziali.

- **Proporzionalità e necessità**: Il trattamento dei dati deve essere adeguato, pertinente e limitato a quanto necessario per il raggiungimento delle finalità dichiarate. I dati non devono essere raccolti in eccesso rispetto a quanto richiesto.
- **Trasparenza**: Gli interessati sono informati in modo chiaro e completo riguardo al trattamento dei loro dati personali, garantendo loro il diritto di essere consapevoli delle modalità e delle finalità del trattamento.
- **Minimizzazione e qualità dei dati**: I dati trattati devono essere essenziali per le finalità perseguite. È essenziale che siano accurati, completi e aggiornati, con misure per correggere o eliminare dati errati o incompleti.
- **Confidenzialità e sicurezza**: I dati devono essere protetti da accessi non autorizzati, garantendo la confidenzialità e l'integrità delle informazioni. L'accesso ai dati è limitato a coloro che sono autorizzati a trattarli per motivi di lavoro.

## 7.1. TIPOLOGIA DEI DATI

Il trattamento potrà avere ad oggetto dati personali comuni, identificativi e di contatto, quali - a titolo esemplificativo e non esaustivo – i dati identificativi (nome, cognome, recapito telefonico, e-mail, data di nascita, curriculum di studi e lavorativo, fotografie allegate al curriculum), altri dati e informazioni relative alle attività di business che intercorrono tra le parti.

METLAC Group raccomanda a tutti gli interessati di non fornire dati particolari ai sensi dell'art. 9 del Regolamento (ovvero dati idonei a rivelare lo stato di salute, la provenienza, le convinzioni religiose, le opinioni politiche, l'orientamento sessuale), fatta salva l'ipotesi in cui i suddetti dati debbano essere conosciuti in ragione dell'instaurazione del rapporto di lavoro, con particolare riferimento all'eventuale appartenenza dell'interessato alle categorie protette e alle eventuali visite mediche finalizzate all'assunzione.

## 7.2. PROTEZIONE DEI DATI E INFORMAZIONI SENSIBILI

- Trattamento lecito, trasparente e limitato alle finalità dichiarate
- Conservazione sicura, accesso controllato, tracciabilità
- Divieto di salvataggio su dispositivi personali o cloud non autorizzati
- Uso di NDA per la condivisione con terze parti
- Diritti dell'interessato: accesso, rettifica, cancellazione, opposizione

## 7.3. FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO

I dati personali raccolti dall'organizzazione a seguito di:

- invio spontaneo o in risposta ad annunci di ricerca e selezione del personale,
- attività lavorativa con scambio di informazioni e documentazione finalizzata al business,
- compilazione di questionari somministrati da METLAC Group finalizzati ad indagini in tema salute, sicurezza, ambiente, Sostenibilità, indice di gradimento dei servizi forniti,
- attività di coinvolgimento e dialogo con gli *Stakeholder* per pratiche legate allo sviluppo sostenibile di METLAC Group e della sua filiera,
- accesso presso gli stabilimenti di METLAC Group e i relativi uffici e per le finalità di controllo degli accessi, di rilevazione della permanenza all'interno delle sedi, di sicurezza dei locali e delle persone in essi presenti,

saranno trattati per le finalità strettamente connesse allo svolgimento delle attività di business, per dar seguito alla richiesta dell'interessato o ricevere l'input per concludere positivamente la transazione in essere.

## 7.4. NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI E CONSEGUENZE DI UN EVENTUALE RIFIUTO AL CONFERIMENTO

La natura del conferimento dei dati personali è da ritenersi facoltativa. A seconda della tipologia di rapporto di collaborazione dello *Stakeholder* coinvolto si potranno verificare e casistiche dettagliate qui di seguito.

- *ASSUNZIONE DEL PERSONALE*: La mancata comunicazione di dati successivamente ed eventualmente richiesti da METLAC Group comporta l'impossibilità di procedere alla verifica dei presupposti per l'assunzione e/o per l'avvio della collaborazione e quindi per l'eventuale instaurazione del rapporto di lavoro.
- *COMUNICAZIONE CON IL PERSONALE*: I dati personali dovranno essere comunicati obbligatoriamente, in quanto necessari per l'instaurazione, perfezionamento e gestione del rapporto di lavoro e per permettere a METLAC Group di effettuare puntualmente gli adempimenti fiscali e previdenziali previsti dalle vigenti normative di legge e adempiere agli obblighi derivanti dalle vigenti normative di legge nonché del CCNL applicato.
- *COMUNICAZIONE CON CLIENTI*: La natura del conferimento dei dati personali è da ritenersi obbligatoria per l'assolvimento degli obblighi contrattuali e precontrattuali. L'eventuale rifiuto a fornire i dati personali necessari potrà determinare l'impossibilità di dare corso ai rapporti contrattuali.
- *COMUNICAZIONE CON I FORNITORI*: La natura del conferimento dei dati personali è da ritenersi obbligatoria per l'assolvimento degli obblighi contrattuali e precontrattuali. L'eventuale rifiuto a fornire i dati personali necessari potrà determinare l'impossibilità di dare corso ai rapporti contrattuali.
- *COMUNICAZIONE CON SOCI*: La natura del conferimento dei dati personali è da ritenersi obbligatoria, mentre è da ritenersi facoltativa laddove il trattamento è soggetto al consenso dell'interessato. L'eventuale rifiuto a fornire i dati personali potrà determinare l'impossibilità per METLAC Group di dare esecuzione agli incarichi.

- *INTERAZIONE CON I VISITATORI*: La natura del conferimento dei dati personali è da ritenersi obbligatoria e l'eventuale rifiuto a fornire i dati personali potrà determinare l'impossibilità di accedere ai locali e uffici di METLAC Group.

### 7.5. MODALITÀ E DURATA DEL TRATTAMENTO

Il trattamento dei dati personali sarà effettuato da personale specializzato e incaricato da METLAC SPA, nei limiti di quanto strettamente necessario, in modo lecito e secondo correttezza, con o senza l'ausilio di mezzi elettronici o comunque automatizzati. Comprenderà tutte le operazioni o il complesso di operazioni necessarie al trattamento in questione, ivi inclusa la registrazione e conservazione presso gli archivi dell'organizzazione (oppure presso i server della *software house*) e verranno adottate misure di sicurezza atte a garantirne la riservatezza ed evitare l'indebito accesso a soggetti terzi o a personale non autorizzato.

I dati potranno essere raccolti anche presso terzi, nel qual caso sarà cura di METLAC Group di procedere tempestivamente ad informare l'interessato/i, come previsto dall'articolo 14 del Regolamento.

I dati saranno conservati per il periodo necessario per il raggiungimento delle finalità per le quali sono stati raccolti e verranno trattati per il periodo di tempo necessario alla gestione dell'attività, della pratica o del processo di interesse, salvo situazioni più particolari quali, ad esempio, l'instaurazione di un rapporto di lavoro, per le quali potranno essere conservati per un periodo uguale o superiore a quello del rapporto di lavoro.

### 7.6. COMUNICAZIONE DEI DATI

I dati personali potranno essere comunicati a dipendenti, impiegati, collaboratori e comunque al solo personale autorizzato da METLAC Group per le finalità del rapporto di business in oggetto.

I dati personali o altre informazioni sensibili potranno essere comunicati a terzi, quali ad esempio fornitori di servizi, consulenti fiscali, consulenti del lavoro e consulenti legali, individuati per le finalità sopraelencate che agiranno quali Responsabili del trattamento ai sensi dell'art. 28 del Regolamento, per conto di METLAC Group e secondo le sue istruzioni.

I suddetti soggetti agiranno quali Titolari Autonomi o Responsabili del trattamento per conto di METLAC Group e secondo le sue istruzioni. L'elenco aggiornato dei Responsabili del Trattamento è disponibile presso la Società capofila di METLAC Group, METLAC SPA, sita in S.S. 35 Bis dei Giovi, 53, CAP 15062 Bosco Marengo (AL), Italia, anche scrivendo all'indirizzo e-mail privacy@metlac.com.

### 7.7. TRASFERIMENTO DEI DATI

I dati personali e altre informazioni sensibili non saranno trasferiti in altri Paesi dell'Unione Europea e in Paesi extra UE (inclusi USA). METLAC Group assicura, sin d'ora, che l'eventuale trasferimento dei dati extra UE avverrà sulla base di adeguate garanzie, in conformità alle disposizioni di legge applicabili e che adotterà tutte le misure necessarie per garantire un'adeguata protezione dei dati personali, quali le *Standard Contractual Clauses* approvate dalla Commissione Europea o altre garanzie equipollenti.

### 7.8. DIRITTI DELL'INTERESSATO

Con la presente METLAC Group informa che, ai sensi degli art. 15-22 del Regolamento il/i soggetto/i interessato/i ha/hanno diritto a esercitare i seguenti diritti:

- di accesso ai dati personali;
- di ricevere conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine;
- di ottenere la rettifica, l'aggiornamento o la cancellazione degli stessi;
- di opporsi al trattamento o di chiederne la limitazione;
- di disporre della portabilità dei dati;
- di revocare il consenso in qualsiasi momento, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prestato prima della revoca e di opporsi al trattamento per finalità di *marketing* e/o profilazione ai sensi dell'art. 21 del Regolamento;
- di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali.

Tali diritti potranno essere esercitati inviando comunicazione scritta al Titolare, METLAC SPA, con sede legale in S.S. 35 Bis dei Giovi, 53, CAP 15062, Bosco Marengo (AL), Italia ovvero all'indirizzo e-mail: privacy@metlac.com.

## 8. RUOLI E RESPONSABILITA' DEGLI ATTORI COINVOLTI

L'organigramma ISMS METLAC Group prevede ruoli specifici:

- CISO (Chief Information Security Officer)
- PdC (Punto di Contatto)
- Sostituto PdC
- Cyber Incident Responder
- Cybersecurity Risk Manager
- Cybersecurity Architect

- Cybersecurity Implementer
- Cyber Legal, Policy and Compliance
- SOCaaS e Threat Intelligence
- ISMS Auditor
- VA/PT Tester
- Digital Forensics Expert
- Cybersecurity Educator

L'organigramma specifico per la Sicurezza delle Informazioni definisce i collegamenti tra questi ruoli.

## 9. FORMAZIONE E CONSAPEVOLEZZA

- Programmi annuali di formazione su cybersecurity e protezione dati
- Simulazioni di phishing e test di reazione
- Materiali informativi su intranet e portale QHSE&S
- KPI di efficacia formativa e coinvolgimento

## 10. MONITORAGGIO, AUDIT E REVISIONE

- Audit indipendenti di prima e seconda parte
- Verifica delle misure implementate e gestione delle non conformità
- Revisione annuale o post-incidenti
- Aggiornamento in caso di modifiche normative o strategiche

## 11. APPROVAZIONE E REVISIONE

Questo documento di Politica è stato redatto da METLAC SPA nel mese di dicembre 2025. La presente versione è stata sottoposta all'approvazione del Consiglio di Amministrazione (CdA) di METLAC Group. La struttura del documento è stata realizzata conformandosi a quanto richiesto dagli standard Europei (*CSRD*).

METLAC Group si riserva di modificare o semplicemente aggiornare il contenuto della presente Politica e delle Informative mirate ai vari soggetti con cui si relaziona, in parte o completamente, a causa di variazioni della normativa applicabile o per esigenze dell'organizzazione. I nuovi documenti per essere considerati validi devono essere sottoposti e approvati dal CdA, quindi comunicati tempestivamente al/ai soggetto/i interessato/i, attraverso i canali di comunicazione aziendali (telematici, sito aziendale, portale SQHSE).

È responsabilità di ciascun Dipartimento aziendale assicurare la conformità con la presente Politica durante il trattamento di informazioni personali e segnalare qualsiasi non conformità o violazione.

## 12. DIFFUSIONE

Questa Politica è pubblicata nella sezione Sostenibilità del sito istituzionale di METLAC Group, insieme al Bilancio di Sostenibilità all'interno del quale sono rendicontate in maniera trasparente le *performance* sociali, ambientali ed economiche della Società [https://www.metlac.com/sostenibilita/].

La politica è:

- Approvata dal CdA METLAC Group
- Pubblicata sul sito istituzionale e sul portale SQHSE
- Comunicata a tutti gli stakeholder
- Inclusa nella documentazione per i nuovi assunti

*CEO*
Pier Ugo Bocchio

*General Manager Italy*
Enrico Buriani

*CRO*
Guido Chiogna

## GLOSSARIO

**2FA**: Autenticazione a due fattori – metodo di accesso sicuro che richiede due elementi di verifica.

**ACN - Autorità garante**: L'organo creato per sorvegliare lo svolgimento di attività economiche realizzate in regime di monopolio o caratterizzate da uno speciale interesse generale.

**Active Directory**: Servizio di directory di Microsoft per la gestione centralizzata di utenti, dispositivi e risorse di rete.

**BitLocker**: Tecnologia Microsoft per la cifratura dei dischi rigidi e la protezione dei dati sui dispositivi.

**CCNL**: Contratto Collettivo Nazionale del Lavoro.

**CISO**: Chief Information Security Officer – responsabile della strategia e dell'architettura di sicurezza informatica.

**Cloud sicuro**: Infrastrutture cloud approvate da METLAC Group (es. Microsoft OneDrive, Teams, Azure) con controlli di sicurezza conformi a ISO/IEC 27017.

**Continuità Operativa**: Business Continuity – capacità dell'organizzazione di continuare a fornire prodotti o servizi a livelli accettabili dopo un incidente.

**CSIRT**: Computer Security Incident Response Team – struttura nazionale per la gestione degli incidenti informatici.

**CSRD**: Corporate Sustainability Reporting Directive – Direttiva europea che stabilisce un nuovo quadro per la rendicontazione non finanziaria delle imprese sul loro impatto ambientale, sociale e di governance.

**Cyber Legal, Policy and Compliance**: Figura professionale che si occupa degli aspetti legali, normativi e di policy in ambito cybersecurity.

**Cyber Incident Responder**: Professionista incaricato di gestire e rispondere agli incidenti di sicurezza informatica.

**Cybersecurity Architect**: Esperto che progetta l'architettura di sicurezza dei sistemi informativi.

**Cybersecurity Educator**: Figura responsabile della formazione e sensibilizzazione del personale sui temi della sicurezza informatica.

**Cybersecurity Implementer**: Professionista che implementa le misure tecniche e organizzative di sicurezza informatica.

**Cybersecurity Risk Manager**: Responsabile della valutazione, gestione e mitigazione dei rischi informatici.

**D.lgs. 101/2018**: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

**D.lgs. 196/2003**: Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679.

**Digital Forensics Expert**: Esperto in analisi forense digitale, incaricato di raccogliere e analizzare prove digitali in caso di incidenti di sicurezza.

**DPO (Data Protection Officer)**: Responsabile della protezione dei dati personali e punto di contatto con l'Autorità Garante.

**Firewall**: Dispositivo o software che controlla e filtra il traffico di rete in ingresso e in uscita secondo regole di sicurezza.

GDPR: 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 e alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, in sintesi "Regolamento generale sulla protezione dei dati".

**IDS/IPS**: Sistemi di rilevamento (IDS) e prevenzione (IPS) delle intrusioni informatiche.

**Informativa**: Complesso di informazioni relative a un determinato argomento e raccolte in un documento, in particolare in materia di trattamento dei dati e delle informazioni sensibili.

**Informazioni personali**: Informazioni riguardanti una persona – anche dette informazioni di identificazione personale (PII) o dati personali – ovvero qualsiasi informazione che possa essere utilizzata per identificare direttamente o indirettamente una persona.

**Informazioni personali sensibili**: Informazioni personali che rivelano condizioni mediche o sanitarie, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza a organizzazioni sindacali o informazioni che riguardano la vita sessuale o l'orientamento sessuale del soggetto in questione.

**IRP (Incident Response Plan)**: Piano operativo per la gestione e la risposta agli incidenti di sicurezza informatica.

**ISMS**: Information Security Management System – Sistema di Gestione della Sicurezza delle Informazioni, conforme a ISO/IEC 27001.

**ISO/IEC 22301**: Standard internazionale per la gestione della continuità operativa.

**ISO/IEC 27001**: Standard internazionale per la gestione della sicurezza delle informazioni.

**ISO/IEC 31000**: Linee guida internazionali per la gestione del rischio.

**Marketing**: Il complesso delle tecniche intese a porre merci e servizi a disposizione del consumatore e dell'utente in un dato mercato nel tempo, luogo e modo più adatti.

**MDM (Mobile Device Management)**: Sistema per la gestione centralizzata e sicura dei dispositivi mobili aziendali.

**NDA**: Non Disclosure Agreement – accordo di riservatezza per la protezione delle informazioni condivise.

**NIS2**: Direttiva (UE) 2022/2555 che impone misure di sicurezza informatica alle entità essenziali e importanti.

**PdC**: Punto di Contatto – figura designata per la comunicazione con le autorità competenti in ambito NIS2.

**Penetration test**: Test di sicurezza che simula attacchi informatici per individuare vulnerabilità nei sistemi.

**Phishing**: Tecnica di attacco informatico che mira a sottrarre dati sensibili tramite messaggi ingannevoli.

**Q81/MAMA**: Software gestionale utilizzato da METLAC per audit, tracciabilità e gestione della sicurezza.

**QHSE&S**: Portale in funzione sulla Intranet aziendale in cui vengono gestite e conservate le documentazioni relative ai sistemi di gestione per la qualità, salute e sicurezza, ambiente e Sostenibilità.

**Server**: In informatica, dispositivo di elevate prestazioni che in una rete fornisce un servizio agli altri elaboratori collegati, detti client.

**SLA (Service Level Agreement)**: Accordo sui livelli di servizio tra fornitore e cliente, con parametri e tempi di risposta definiti.

**SOCaaS**: Security Operations Center as a Service – servizio esterno per il monitoraggio e la risposta agli incidenti informatici.

**Software house**: Azienda che si occupa dell'elaborazione e della commercializzazione di programmi informatici.

**Sviluppo Sostenibile**: Adozione di modalità capaci di rispondere ai bisogni del presente e del futuro, conciliando salute ambientale, equità sociale e vitalità economica.

**Stakeholder**: Individuo, gruppo o organizzazione che ha un interesse o è influenzato, direttamente o indirettamente, dalle attività, dalle decisioni o dai risultati di un'azienda.

**Standard Contractual Clauses**: Documenti standard pre-approvati che contengono dei requisiti minimi da rispettare nel trasferimento dei dati all'estero.

**Trattamento**: Qualsiasi operazione o serie di operazioni condotte sulle informazioni personali, anche attraverso mezzi automatici e digitalizzati.

**VA/PT Tester**: Esperto in Vulnerability Assessment e Penetration Testing – verifica la robustezza dei sistemi contro eventuali attacchi.

**VPN (Virtual Private Network)**: Rete privata virtuale che consente connessioni sicure e cifrate su reti pubbliche.

**WPA2/WPA3**: Standard di sicurezza per la protezione delle reti Wi-Fi.