TERMINI E CONDIZIONI DI ABBONAMENTO SaaS E LICENZA D'USO

Piattaforma web per la gestione degli obblighi AML e processi connessi

"AML GUARDIAN"

0. Come si conclude il Contratto online

0.1 Il presente documento ("**Contratto**") disciplina l'uso della piattaforma AML GUARDIAN ("**Piattaforma**") erogata in modalità SaaS.

0.2 Il Contratto si conclude online quando il soggetto che acquista ("**Cliente**") completa l'ordine sul sito e seleziona le caselle di accettazione richieste (inclusa, ove prevista, l'accettazione specifica ex artt. 1341–1342 c.c.).

0.3 I dati identificativi del Cliente (ragione sociale, P.IVA/C.F., sede, PEC/e-mail, nominativo del referente) sono quelli inseriti in fase di acquisto e/o nella console amministrativa del Cliente e formano parte integrante dell'ordine ("**Ordine Online**").

1. Parti

1.1 **Fornitore**: **L&CM Società tra Avvocati Srl**, con sede in Via di Vittorio 2 – 20019 Settimo Milanese, C.F./P.IVA 10399790962, in persona del legale rappresentante p.t. ("**L&CM**" o "**Fornitore**").

1.2 **Cliente**: il soggetto che acquista il Servizio tramite Ordine Online.

2. Premesse e documenti contrattuali

2.1 Il Cliente utilizza la Piattaforma per supportare l'organizzazione, tracciabilità e gestione di attività e documentazione connesse ai propri obblighi AML, coerentemente con la normativa applicabile al Cliente e con i propri presidi interni.

2.2 Sono parte integrante del Contratto:

- **Allegato A Offerta economica / Piano e Metriche**

- **Allegato B – Misure di sicurezza**
- **Allegato C – DPA**

3. Definizioni essenziali

3.1 **Servizio**: accesso e utilizzo della Piattaforma SaaS, inclusi aggiornamenti correttivi e di sicurezza, manutenzione ordinaria e supporto.

3.2 **Utenti**: persone fisiche autorizzate dal Cliente ad accedere alla Piattaforma sotto la responsabilità del Cliente.

3.3 **Dati del Cliente**: dati e contenuti caricati o generati dal Cliente/Utenti tramite la Piattaforma (inclusi documenti e fascicoli AML), nonché log e metadati collegati all'uso, nei limiti del Servizio.

4. Oggetto – Abbonamento e licenza d'uso SaaS

4.1 Il Fornitore concede al Cliente una licenza d'uso **non esclusiva**, **non trasferibile**, **non sublicenziabile** di accesso e utilizzo della Piattaforma per la durata dell'abbonamento.

4.2 Servizi professionali e moduli opzionali (setup, parametrizzazione, formazione dedicata, migrazioni, export assistito) sono erogati se acquistati con Ordine Online o preventivo accettato.

4.3 L&CM, ancorché società tra avvocati, opera ai sensi del presente Contratto esclusivamente quale soggetto che commercializza e mette a disposizione una piattaforma tecnologica in modalità Software as a Service (SaaS).

4.4 L'attività svolta da L&CM in esecuzione del presente Contratto non costituisce e non può in alcun modo essere qualificata come attività di consulenza, assistenza o prestazione legale, né individuale né professionale.

4.5 I contenuti, le funzionalità, gli strumenti e gli eventuali output generati dalla Piattaforma hanno natura esclusivamente informativa, tecnica e/o automatizzata e non sostituiscono in alcun modo il parere, la consulenza o l'intervento di un professionista legale abilitato.

4.6 L'utilizzo della Piattaforma non determina l'instaurazione di alcun rapporto professionale di natura legale tra L&CM e l'Utente, restando quest'ultimo l'unico responsabile delle decisioni assunte e dell'uso delle informazioni ottenute tramite la Piattaforma.

5. Attivazione, account, Utenti e credenziali

5.1 L'accesso avviene mediante credenziali e/o strumenti di autenticazione.

5.2 Il Cliente è responsabile di: (i) corretta gestione delle credenziali; (ii) assegnazione/revoca accessi; (iii) operato degli Utenti.

5.3 Il Cliente segnala tempestivamente accessi non autorizzati o incidenti di sicurezza noti.

6. Limitazioni d'uso

6.1 È vietato: copiare, decompilare, disassemblare, reverse engineering; aggirare misure di sicurezza; uso illecito; accesso a terzi non autorizzati; estrazioni massive in violazione di limiti tecnici/contrattuali.

7. Clausole essenziali su compliance AML

7.1 La Piattaforma è **strumento di supporto** e non sostituisce gli obblighi del Cliente, né garantisce di per sé la piena conformità AML in ogni caso concreto.

7.2 Il Cliente resta unico responsabile di policy, processi, configurazioni, completezza/qualità dati, decisioni e valutazioni, e conservazione secondo gli obblighi applicabili alla propria attività.

7.3 Eventuali contenuti/modelli/linee guida hanno finalità informativa/operativa e non costituiscono garanzia di risultato.

8. Configurabilità e parametri – Responsabilità del Cliente

8.1 Regole, soglie, workflow, check-list e template (anche se preimpostati) sono configurabili e devono essere verificati e mantenuti dal Cliente.

8.2 Salvo servizi professionali espressamente acquistati, il Fornitore non è responsabile della corretta impostazione/aggiornamento dei parametri né delle conseguenze di configurazioni errate o non aggiornate.

8.3 Gli output della Piattaforma costituiscono supporto operativo e non determinazioni vincolanti.

9. Terze parti, banche dati esterne e integrazioni

9.1 La Piattaforma può integrarsi con provider terzi.

9.2 Il Cliente è responsabile di titolo, basi giuridiche e rispetto dei termini del provider.

9.3 Salvo dolo o colpa grave, il Fornitore non risponde di indisponibilità/errori imputabili a terzi; coopera ragionevolmente per mitigare impatti compatibilmente con limiti tecnici ed economici.

10. Conservazione, export e cessazione

10.1 Il Fornitore garantisce accessibilità e disponibilità dei Dati del Cliente **solo in costanza di abbonamento attivo e pagato**, salvo manutenzioni programmate o disservizi non imputabili.

10.2 Alla cessazione (scadenza senza rinnovo o risoluzione), il Cliente perde il diritto di accesso alla Piattaforma.

10.3 **Export autonomo**: fino alla cessazione effettiva, il Cliente può esportare autonomamente nei limiti tecnici indicati in Documentazione.

10.4 **Export assistito**: se richiesto entro **60 giorni** dalla cessazione, il Fornitore effettua export assistito a pagamento alle condizioni dell'Allegato A, in formato [ZIP/PDF/CSV/JSON] o altro formato tecnicamente ragionevole concordato.

10.5 Decorso il termine di 60 giorni senza export autonomo o richiesta/esecuzione export assistito (incluso pagamento), il Fornitore può procedere alla cancellazione dei Dati del Cliente dagli ambienti di produzione; copie di backup possono permanere per un periodo tecnico limitato fino a sovrascrittura, con accesso ristretto.

10.6 Salvo pattuizione scritta, la Piattaforma non fornisce conservazione sostitutiva a norma (CAD/AgID).

11. Corrispettivi, fatturazione e pagamenti

11.1 Canoni, metriche e servizi extra sono quelli dell'**Allegato A** associato all'Ordine Online.

11.2 Fatturazione **annuale anticipata**, salvo diversa indicazione nell'Ordine Online; pagamento secondo i metodi e termini indicati in checkout/fattura.

11.3 In caso di ritardo: interessi ex D.Lgs. 231/2002 e facoltà di sospendere il Servizio previa comunicazione.

12. SLA, manutenzione e supporto

13.1Manutenzioni urgenti per sicurezza/stabilità possono essere svolte senza preavviso ove necessario.

13. Proprietà intellettuale

13.1 Piattaforma, Documentazione, marchi e diritti IP restano del Fornitore e/o licenzianti.

13.2 Il Cliente resta titolare dei propri Dati.

14. GDPR e sicurezza

14.1 Le Parti si impegnano al rispetto del GDPR e normativa applicabile.

14.2 Il Cliente è **Titolare** e il Fornitore è **Responsabile** ai sensi dell'Allegato C (DPA).

14.3 Misure di sicurezza: Allegato B.

14.4 Il Cliente è responsabile di informative, basi giuridiche, autorizzazioni e legittimità dei dati caricati e delle consultazioni verso banche dati esterne.

14.5 Il Cliente prende atto che il Fornitore si avvale di **4Sigma Srl** quale subfornitore tecnico; 4Sigma è indicata nel DPA come **sub-responsabile**.

15. Subfornitori

15.1 Il Fornitore può avvalersi di subfornitori per erogare il Servizio (sviluppo, hosting, ticketing, monitoring), restando responsabile verso il Cliente.

15.2 Per subfornitori che trattano dati personali come sub-responsabili, si applica il DPA (Allegato C) inclusi elenco e diritto di opposizione.

16. Riservatezza

16.1 Ciascuna Parte mantiene riservate le informazioni confidenziali dell'altra e le usa solo per eseguire il Contratto.

16.2 Durata: per tutta la vigenza e **5 anni** dopo la cessazione (salvo segreti industriali finché tali).

17. Garanzie

17.1 Il Fornitore eroga il Servizio con diligenza professionale.

17.2 Sono escluse garanzie implicite nei limiti di legge.

17.3 È esclusa qualsiasi garanzia di "compliance automatica" AML.

18. Manleva

18.1 Il Fornitore manleva il Cliente da pretese di terzi per violazione di diritti IP sulla Piattaforma, alle condizioni di notifica tempestiva, gestione difesa e cooperazione.

18.2 Il Cliente manleva il Fornitore per pretese derivanti da Dati del Cliente illeciti, violazioni privacy, uso non conforme o illegittimità delle interrogazioni a banche dati esterne.

19. Limitazione di responsabilità

19.1 Salvo dolo o colpa grave e limiti inderogabili, il Fornitore non risponde di danni indiretti o consequenziali (perdita profitto, interruzione attività, perdita opportunità).

19.2 La responsabilità complessiva del Fornitore per danni diretti è limitata ai corrispettivi pagati dal Cliente nei **12 mesi** precedenti l'evento.

19.3 Restano ferme le responsabilità non limitabili per legge.

20. Durata e rinnovo (web-only, non automatico)

20.1 Il Contratto ha durata **annuale (12 mesi)** dalla data di attivazione o dalla data indicata nell'Ordine Online ("Periodo di Abbonamento").

20.2 In prossimità della scadenza, indicativamente non oltre **60 giorni** prima, il Fornitore può proporre il rinnovo per ulteriori 12 mesi.

20.3 Il rinnovo **non è automatico**: si perfeziona solo con accettazione online del Cliente (nuovo Ordine Online o accettazione della proposta di rinnovo). In mancanza, il Contratto cessa alla scadenza e si applica l'art. 10.

21. Risoluzione

21.1 Clausola risolutiva espressa ex art. 1456 c.c. per: mancato pagamento, violazioni art. 6 (limitazioni), violazioni riservatezza, violazioni sicurezza gravi, uso illecito.

21.2 In caso di cessazione si applicano art. 10 e DPA.

22. Comunicazioni

22.1 Comunicazioni formali via PEC del Fornitore e PEC/e-mail del Cliente indicate nell'Ordine Online o nell'account amministratore.

23. Legge applicabile e foro

23.1 Legge italiana. Foro esclusivo: Milano, salvo norme inderogabili.

24. Disposizioni finali e prevalenza DPA

24.1 Gli Allegati sono parte integrante.

24.2 Nullità parziale: le restanti clausole restano valide.

24.3 Modifiche: solo per iscritto, salvo aggiornamenti tecnici/di sicurezza e/o SLA comunicati al Cliente.

24.4 In caso di conflitto tra Contratto e DPA su aspetti privacy, **prevale il DPA**.

25. Accettazioni specifiche (artt. 1341–1342 c.c.)

25.1 Il Cliente dichiara di approvare specificamente le clausole: **6, 7, 8, 9, 10, 11, 12, 17, 18, 19, 20, 21, 23**.

25.2 L'approvazione avviene tramite checkbox separata in fase di acquisto.

ALLEGATO A – Offerta economica / Piano e Metriche (web)

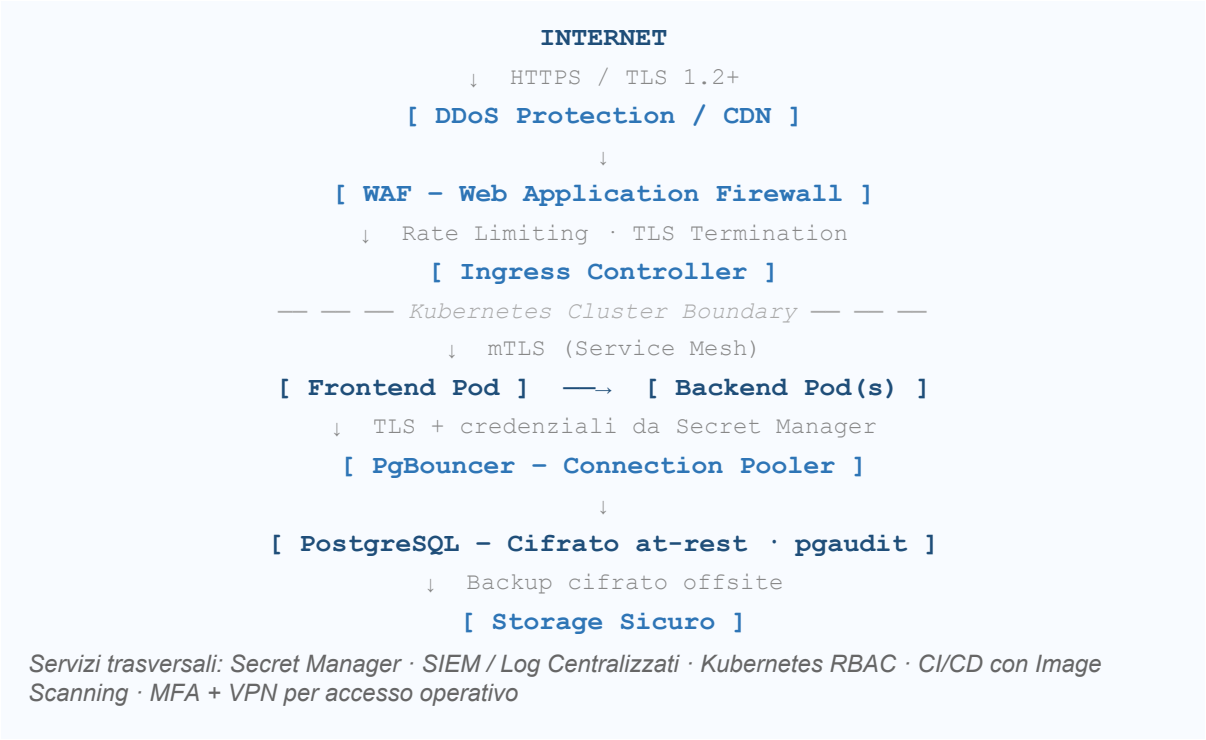
Per quel che riguarda le condizioni economiche si rimanda all'apposita pagina presente sul sito: https://amlguardian.it/prezzi/

Sono disponibili diverse convenzioni che prevedono un tariffario scontato, l'elenco completo delle convenzioni attive è disponibile a questo indirizzo:

https://amlguardian.it/convenzioni/

ALLEGATO B – Misure di sicurezza (schema)

Di seguito è rappresentata la struttura logica dei livelli di sicurezza adottati:



3. Misure di Sicurezza per Livello

3.1 Sicurezza dell'Infrastruttura

Kubernetes Cluster
Aggiornamento periodico del cluster e dei nodi (patch management pianificato)
Accesso al control plane limitato tramite RBAC (Role-Based Access Control)
Network Policies per isolare i namespace e limitare il traffico tra pod
API server non esposto pubblicamente: accesso solo via VPN o IP allowlist
Audit logging del cluster abilitato e centralizzato

Nodi Worker
OS hardening secondo CIS Benchmark
Accesso SSH disabilitato o gestito tramite chiavi con rotazione periodica
Aggiornamenti automatici delle patch di sicurezza del sistema operativo

3.2 Sicurezza dei Container

Hardening delle Immagini Docker
Immagini basate su distribuzioni minimali (distroless / alpine)
Scansione automatica delle vulnerabilità in pipeline CI/CD (es. Trivy, Snyk)
Firma delle immagini e verifica dell'integrità (Docker Content Trust / Cosign)
Container eseguiti come utente non-root
Filesystem del container configurato in modalità read-only ove possibile
Capabilities Linux ridotte al minimo necessario (drop ALL, add selettivo)
Modalità privilegiata disabilitata (privileged: false)
Limiti di risorse (CPU/memory limits) definiti per ogni container

3.3 Sicurezza della Rete

Protezione del Traffico di Rete
Traffico esterno gestito tramite Ingress Controller con TLS terminato (cert. Let's Encrypt o CA aziendale)
Comunicazioni interne tra servizi cifrate con mTLS tramite Service Mesh (Istio / Linkerd)
Separazione logica in namespace Kubernetes dedicati (es. frontend, backend, database)
Network Policies Kubernetes per whitelist del traffico tra pod
WAF (Web Application Firewall) davanti all'Ingress per protezione OWASP Top 10

- Protezione DDoS attiva (es. Cloudflare, AWS Shield o equivalente)

3.4 Sicurezza dei Dati

Dati in Transito (In Transit)
TLS 1.2+ obbligatorio su tutte le comunicazioni esterne
mTLS per le comunicazioni interne service-to-service all'interno del cluster

Dati a Riposo (At Rest)
Cifratura del volume di storage dei pod (es. EBS cifrato, PVC con encryption)
Cifratura del database PostgreSQL a livello di volume
Cifratura a livello applicativo dei dati sensibili (PII) prima della persistenza

Gestione dei Segreti
Nessuna credenziale hardcoded nelle immagini Docker o nei manifest Kubernetes
Utilizzo di un Secret Manager dedicato (es. HashiCorp Vault, AWS Secrets Manager, KMS)
Rotazione automatica delle credenziali del DB e delle API key
Kubernetes Secrets cifrati a riposo tramite KMS provider

3.5 Sicurezza del Database PostgreSQL

Protezione del Database
Porta 5432 non esposta pubblicamente: accesso consentito solo ai pod applicativi autorizzati
Autenticazione con credenziali dedicate per ciascun servizio (principio del minimo privilegio)
TLS abilitato su tutte le connessioni al database

- Audit log delle query tramite estensione pgaudit
- Backup cifrati e memorizzati in storage offsite con verifica periodica del ripristino
- Connection pooling tramite PgBouncer per ridurre la superficie d'attacco e gestire le connessioni
- Network Policy Kubernetes che limita l'accesso al DB ai soli namespace autorizzati

3.6 Sicurezza Applicativa

Application Security
Gestione sicura delle sessioni: token JWT con scadenza, refresh token rotation
Protezione contro CSRF, XSS, SQL Injection e attacchi OWASP Top 10
Rate limiting e throttling sulle API pubbliche
Validazione e sanitizzazione degli input lato server
Dependency scanning (SCA) e analisi statica/dinamica del codice (SAST/DAST) in CI/CD
Header di sicurezza HTTP configurati (CSP, HSTS, X-Frame-Options, X-Content-Type-Options)

3.7 Identity & Access Management

Controllo degli Accessi
Autenticazione multi-fattore (MFA) obbligatoria per tutti gli accessi amministrativi
Principio del minimo privilegio applicato a tutti i ruoli (Kubernetes RBAC, DB roles, IAM cloud)
Service Account Kubernetes con permessi minimi e token a breve scadenza
Accesso all'ambiente di produzione solo tramite VPN + bastion host (nessun accesso diretto)
Revisione periodica dei permessi e rimozione degli accessi non necessari

3.8 Monitoraggio, Logging e Incident Response

Osservabilità e Risposta agli Incidenti
Centralizzazione dei log applicativi e di sistema (es. ELK Stack, Loki + Grafana)
Alerting su anomalie: tentativi di login falliti, spike di traffico, comportamenti insoliti
SIEM per la correlazione degli eventi di sicurezza
Procedure di Incident Response documentate e testate periodicamente
Penetration test periodici (frequenza minima: annuale) con report documentati
Vulnerability Disclosure Policy pubblica

4. Riepilogo delle Misure per Categoria

Categoria	Misura Principale
Infrastruttura	Kubernetes RBAC, OS hardening, patch management
Container	Immagini minimali, scansione CVE, non-root, read-only FS
Rete	TLS 1.2+, mTLS, WAF, Network Policies, DDoS protection
Dati in transito	TLS obbligatorio su tutti i canali esterni e interni
Dati a riposo	Cifratura volumi, DB cifrato, cifratura applicativa PII
Segreti	Secret Manager, nessuna credenziale hardcoded, rotazione automatica
Database	Accesso limitato, TLS, pgaudit, backup cifrati, PgBouncer
Applicazione	OWASP Top 10, rate limiting, SAST/DAST, header sicurezza
IAM	MFA, minimo privilegio, VPN + bastion, revisione accessi
Monitoraggio	Log centralizzati, SIEM, alerting, Incident Response, pentest

5. Riferimenti Normativi e Standard

Le misure descritte nel presente allegato sono state definite in conformità ai seguenti standard e normative:

- Regolamento (UE) 2016/679 – GDPR, art. 25 e art. 32 (misure tecniche e organizzative adeguate)
- CIS Kubernetes Benchmark – Center for Internet Security
- OWASP Top 10 – Open Web Application Security Project
- NIST Cybersecurity Framework (CSF) v2.0
- ISO/IEC 27001:2022 – Sistemi di gestione della sicurezza delle informazioni

ALLEGATO C – DPA

(Cliente=Titolare, L&CM=Responsabile, 4Sigma=Sub-responsabile)

1. Parti e ruoli

1.1 **Titolare**: il Cliente.

1.2 **Responsabile**: **L&CM Società tra Avvocati Srl**.

1.3 **Sub-responsabile già autorizzato**: **4Sigma Srl** (sub-processor) per attività tecniche necessarie all'erogazione della Piattaforma.

1.4 Il presente DPA disciplina il trattamento dei dati personali effettuato dal Responsabile per conto del Titolare in esecuzione del Contratto.

2. Oggetto, durata, natura e finalità

2.1 Oggetto: erogazione SaaS della Piattaforma e servizi connessi (supporto, manutenzione, sicurezza, backup, export assistito).

2.2 Durata: per la durata del Contratto e fino a restituzione/cancellazione ai sensi dell'art. 10 del presente DPA e dell'art. 11 del Contratto.

2.3 Operazioni: raccolta/registrazione, organizzazione, conservazione, consultazione, estrazione/export, cancellazione, backup/ripristino, logging e audit trail.

3. Istruzioni del Titolare

3.1 Il Responsabile tratta i dati personali solo su istruzioni documentate del Titolare (Contratto, DPA, Documentazione).

3.2 Se un'istruzione appare illecita, il Responsabile informa il Titolare.

4. Categorie di dati e interessati

Come da **Appendice 1**. Possibile presenza di dati ex art. 9 e/o 10 GDPR in funzione dell'[9]uso del Titolare.

5. Sicurezza

5.1 Misure adeguate ex art. 32 GDPR come da **Appendice 2**.

5.2 Personale autorizzato vincolato a riservatezza.

6. Assistenza al Titolare

6.1 Supporto ragionevole per richieste interessati (artt. 15–22) nei limiti tecnici del Servizio.

6.2 Supporto informativo per DPIA/consultazione preventiva (artt. 35–36) ove ragionevolmente disponibile.

7. Data breach

7.1 Notifica al Titolare senza ingiustificato ritardo e, ove possibile, **entro 48 ore** dalla scoperta.

7.2 Contenuti: natura, categorie/volume stimato, conseguenze probabili, misure adottate/proposte, contatto.

8. Sub-responsabili (inclusa 4Sigma Srl)

8.1 Il Titolare conferisce autorizzazione generale alla nomina di sub-responsabili necessari.

8.2 4**Sigma Srl è sin da ora autorizzata** come sub-responsabile per sviluppo/manutenzione/gestione tecnica della Piattaforma e supporto tecnico, nei limiti delle istruzioni del Responsabile e del Titolare.

8.3 Modifiche all'elenco: preavviso **30 giorni**; opposizione motivata entro 30 giorni; cooperazione per alternative; in mancanza, recesso limitatamente alla parte impattata o dal Contratto se essenziale, senza penali ulteriori rispetto ai corrispettivi maturati.

8.4 Il Responsabile stipula con ogni sub-responsabile un accordo con obblighi non meno rigorosi (art. 28(4) GDPR) e resta responsabile verso il Titolare.

9. Trasferimenti extra SEE

9.1 Vietati salvo quanto indicato in Appendice 3 e con garanzie adeguate (SCC o equivalenti) ove applicabili.

10. Fine trattamento: export e cancellazione

10.1 Coerentemente con l'art. 11 del Contratto: export autonomo fino alla cessazione; export assistito richiedibile entro **60 giorni**; decorso il termine, cancellazione da produzione (salvi obblighi di legge).

10.2 Backup: permanenza tecnica limitata fino a sovrascrittura, con accesso ristretto e misure adeguate.

11. Prevalenza

11.1 In caso di conflitto tra DPA e Contratto su aspetti privacy, prevale il DPA.

Accettazione online: il DPA si intende accettato con la checkbox dedicata in fase di acquisto.

APPENDICE 1 – Descrizione del trattamento

- Interessati: Utenti del Cliente; clienti/controparti; legali rappresentanti, delegati, titolari effettivi; altri soggetti presenti nei fascicoli AML.
- Dati: identificativi/contatto; documenti (ID, visure); dati economico-professionali; valutazioni rischio; anomalie/alert; note/motivazioni; log accessi; eventuali dati PEP/sanzioni se inseriti/gestiti dal Cliente o via provider.
- Finalità: erogazione SaaS, supporto, manutenzione, sicurezza/continuità, export.

APPENDICE 2 – Misure di sicurezza (baseline)

RBAC/gestione accessi, TLS, logging/audit trail, backup e test ripristino, segregazione ambienti/tenant, vulnerability management, incident response, least privilege, gestione segreti/chiavi.

APPENDICE 3 – Sub-responsabili (elenco minimo)

- **4Sigma Srl** – Paese: Italia – Finalità: sviluppo/manutenzione/gestione tecnica e supporto tecnico Piattaforma
- Provider hosting/cloud: Digital Ocean – Paese: Germania
- Ticketing/support: 4Sigma Srl – Paese: Italia
- Monitoring/log: 4Sigma Srl – Paese: Italia

Informativa ex art. 13 Reg. UE 2016/679

(allegato al Contratto di abbonamento SaaS e licenza d'uso della Piattaforma web per la gestione dei fascicoli AML e processi connessi)

L&CM Società tra Avvocati S.r.l., in qualità di Titolare del trattamento, desidera informarVi che il Regolamento UE 2016/679 prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Vostra riservatezza e dei Vostri diritti.

Ai sensi dell'articolo 13 del Regolamento UE 2016/679, pertanto, Vi forniamo le seguenti informazioni:

---

1. Identità e dati di contatto del titolare/responsabile del trattamento

L&CM Società tra Avvocati S.r.l. (di seguito "**L&CM**"), società a responsabilità limitata tra avvocati, ha per oggetto esclusivo l'esercizio, da parte dei soli soci iscritti all'ordine degli avvocati, della professione propria degli iscritti all'ordine degli avvocati.

Nell'ambito di tale attività:

- **L&CM tratta i dati personali in qualità di Titolare del Trattamento** per le finalità indicate al punto 3, connesse alla gestione e all'esecuzione del rapporto contrattuale relativo alla Piattaforma SaaS, nonché agli adempimenti di legge.
- Inoltre, **nei casi in cui il Cliente utilizzi la Piattaforma caricando dati personali di terzi** (es.
- anagrafiche, documenti e fascicoli AML), **L&CM può essere nominata Responsabile del Trattamento dal Cliente** (Titolare del trattamento) ai sensi dell'art. 28 del Regolamento, secondo quanto previsto nel **DPA (Allegato C)** al Contratto.

L&CM ha sede a **Milano – Via Colonnetta, 5**, nella persona del legale rappresentante pro-tempore.

---

2. Dati di contatto del Responsabile della Protezione dei Dati

L&CM ha nominato un **Responsabile della Protezione dei dati (DPO)** che può essere contattato oltre che presso la sede della Società anche a mezzo posta elettronica all'indirizzo:

contatti.dpo@abcd.space

---

3. Finalità e base giuridica del Trattamento

I dati da Voi forniti (e/o generati dall'utilizzo della Piattaforma) verranno trattati per le seguenti finalità:

- **esecuzione del Contratto SaaS**, inclusa attivazione e gestione dell'account, erogazione del Servizio, assistenza e supporto, gestione richieste e comunicazioni di servizio;
- **gestione contabile ed amministrativa** dei rapporti contrattuali (fatturazione, pagamenti, gestione crediti, adempimenti fiscali);
- **sicurezza e continuità del Servizio**, inclusi log tecnici, monitoraggio, prevenzione abusi, gestione incidenti e data breach, nonché backup e ripristino;
- **adempimento di obblighi di legge** e tutela dei diritti del Titolare (es. gestione contestazioni, difesa in giudizio);
- **elaborazioni statistiche** e analisi aggregate sull'uso della Piattaforma (ove possibile in forma aggregata e/o con misure di minimizzazione).

Base giuridica del trattamento:

- per le finalità di cui ai primi due punti: **esecuzione del contratto** e/o misure precontrattuali (art. 6, par. 1, lett. b) GDPR);
- per sicurezza, prevenzione abusi e tutela dei diritti: **legittimo interesse** del Titolare (art. 6, par. 1, lett. f) GDPR), bilanciato con i diritti degli interessati;
- per adempimenti di legge: **obbligo legale** (art. 6, par. 1, lett. c) GDPR).

Il trattamento sarà effettuato principalmente mediante elaborazione elettronica e strumenti informatici.

Nota: per i dati personali eventualmente caricati dal Cliente nella Piattaforma relativi a terzi (es. clienti/controparti/titolari effettivi), le finalità e basi giuridiche del trattamento sono determinate dal **Cliente** in qualità di **Titolare del trattamento**, mentre L&CM opera, per tali dati, quale **Responsabile del trattamento** secondo il DPA.

4. Eventuali categorie di destinatari dei dati personali

I dati da Voi forniti potranno formare oggetto di ogni altra opportuna operazione relativa al conseguimento delle predette finalità anche per mezzo:

- di soggetti specificamente autorizzati quali consulenti, dipendenti e altri collaboratori a ciò abilitati per i trattamenti necessari o connessi alle finalità in parola;
- di terzi che svolgono o forniscono specifici servizi strettamente funzionali alle finalità in parola, quali:
    - **fornitori di servizi informatici e tecnologici** (es. manutenzione, assistenza, ticketing, monitoraggio, infrastruttura/hosting e relativi servizi);
    - **4Sigma Srl** (subfornitore tecnico) per attività di sviluppo/manutenzione/gestione tecnica e supporto della Piattaforma, nei limiti delle istruzioni e degli obblighi contrattuali e privacy applicabili;
    - soggetti che svolgono servizi contabili/fiscali, istituti di credito e fornitori di servizi di pagamento;
    - consulenti legali e assicurazioni, ove necessario;

il tutto nel rispetto delle disposizioni di legge in materia di sicurezza dei dati. L'elenco nominativo dei soggetti appartenenti alle predette categorie è disponibile presso la sede della Società.

---

5. Tempi di conservazione dei dati personali

I dati da Voi forniti saranno conservati da L&CM per il tempo necessario al perseguimento delle finalità indicate al punto 3.

In particolare:

- i dati relativi alla gestione del rapporto contrattuale e amministrativo-contabile saranno conservati per il tempo necessario all'esecuzione del Contratto e, successivamente, per i termini previsti dalla normativa applicabile (es. obblighi civilistici e fiscali);
- i dati tecnici e log di sicurezza saranno conservati per un periodo coerente con le finalità di sicurezza e con le misure indicate nella Documentazione e/o nelle policy interne, nel rispetto dei principi di minimizzazione;
- per i **Dati del Cliente** presenti nella Piattaforma (inclusi documenti e fascicoli AML), la conservazione e cancellazione avvengono secondo quanto previsto dal Contratto (export e cessazione) e dal DPA: in particolare, in caso di cessazione del Servizio, il Cliente può effettuare export autonomo fino alla cessazione ed eventualmente richiedere export assistito entro 60 giorni; decorso tale termine, i dati potranno essere cancellati dagli ambienti di produzione, ferma la possibile permanenza di copie di backup per un periodo tecnico limitato fino a sovrascrittura.

In ogni caso i tempi di conservazione non potranno superare i termini di legge o contrattuali previsti per le singole categorie degli stessi.

---

6. Diritti dell'Interessato

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere l'accesso ai propri dati personali, la rettifica o la cancellazione degli stessi ai sensi degli articoli 15, 16 e 17 del Reg. UE 2016/679.

Ai sensi degli articoli 18, 20 e 21 del medesimo Regolamento gli interessati hanno inoltre il diritto di chiedere la limitazione del trattamento, la portabilità dei dati che li riguardano (se applicabile) nonché di opporsi, per motivi legittimi, al loro trattamento.

I diritti di cui sopra potranno essere esercitati:

- **nei confronti del Cliente** (Titolare del trattamento), per i dati trattati tramite la Piattaforma nell'ambito dei processi AML del Cliente; e/o
- **nei confronti di L&CM**, in relazione ai trattamenti dalla stessa effettuati in qualità di Titolare (es. gestione del rapporto contrattuale, fatturazione, comunicazioni di servizio, sicurezza e tutela dei diritti), a mezzo:

  – e-mail all'indirizzo: **info@l-cm.it**

  – posta ordinaria: **L&CM Società tra Avvocati S.r.l. – Via Colonnetta, 5 – Milano**.

Ai medesimi recapiti è altresì possibile richiedere ulteriori informazioni, ivi compresi i riferimenti degli eventuali responsabili/sub-responsabili del trattamento.

---

7. Reclamo ad una Autorità di Controllo

Se la risposta ad un'istanza con cui l'interessato ha esercitato uno o più dei diritti di cui sopra non dovesse pervenire nei tempi indicati o non dovesse risultare soddisfacente, l'interessato potrà far valere i suoi diritti dinanzi all'Autorità Giudiziaria o rivolgendosi al **Garante per la Protezione dei Dati Personali**.