

Procedura e Policy interna per l'uso degli strumenti di IA in Lexant

Premessa normativa e campo di applicazione	1
Strumenti autorizzati e titolarità degli accessi	1
Principi di utilizzo.....	1
Attività consentite/sconsigliate/vietate.....	2
Ruoli e responsabilità	3
Formazione e AI literacy	3
Tracciabilità e audit.....	3
Data protection e trasferimenti.....	3
Gestione incidenti.....	3
Revisione.....	3

Premessa normativa e campo di applicazione

La presente procedura disciplina l'uso di strumenti di IA in Lexant SBtA a r.l. - di seguito "**Lexant**" o "**Studio**"-, in coerenza con:

- (i) la **Legge 132/2025**, in particolare l'art. 13 sulle "*professioni intellettuali*", che impone di informare il cliente sui sistemi IA utilizzati e circoscrive l'IA ad attività strumentali e di supporto, con prevalenza del lavoro intellettuale del professionista;
- (ii) l'**AI Act** (Reg. (UE) 2024/1689), in particolare l'art. 4 (*AI literacy*) e l'art. 50 (trasparenza verso gli interessati e marcatura/indicazione dei contenuti sintetici ove rilevante).

Restano ovviamente fermi il GDPR e il segreto professionale.

Strumenti autorizzati e titolarità degli accessi

Gli strumenti autorizzati in Lexant sono:

- (i) ChatGPT Teams;
- (ii) Lexroom;
- (iii) a Gamma;
- (iv) DeepL.

Gli accessi sono assegnati ai Capi Divisione, che possono autorizzarne l'utilizzo agli Avvocati del team. L'uso di account personali è vietato; ogni attività deve avvenire tramite credenziali dello Studio. Le impostazioni privacy vanno configurate secondo il principio di minima esposizione dei dati (es. disattivazione di eventuali opzioni di "*miglioramento del modello*" ove presenti; impiego di versioni business/enterprise che non utilizzano per training i dati aziendali, secondo le policy del fornitore). Per OpenAI, le pagine istituzionali indicano che i dati "*business/enterprise*" non sono utilizzati per addestrare i modelli salvo opt-in esplicito. DeepL pubblica impegni di sicurezza/conformità e un Trust Center dedicato; Lexroom dichiara che i dati caricati non sono usati per l'addestramento e restano segregati; Gamma documenta prassi privacy e controlli. Tali profili devono essere verificati periodicamente dall'IT/Compliance.

Principi di utilizzo

(a) Supporto, non sostituzione.

Gli strumenti IA si impiegano quando il professionista ha già l'impostazione della risposta e intende approfondire, verificare o velocizzare passaggi (ricerca, riordino documenti, prime bozze, traduzioni). La decisione, la strategia e la

responsabilità restano sempre del professionista. Ciò riflette quanto prevede l'art. 13 Legge 132/2025.

(b) Verifica umana obbligatoria.

Ogni output va verificato criticamente, con controllo di accuratezza giuridica, attualità delle fonti e assenza di allucinazioni/omissioni.

(c) Minimizzazione dei dati.

Si evitano riferimenti identificativi non necessari; si preferiscono prompt “sterilizzati” (pseudonimizzazione, mascheramento nomi, rimozione di dati sensibili) e si caricano solo documenti indispensabili allo scopo.

(d) Segreto professionale e riservatezza.

Mai caricare, nelle versioni consumer degli strumenti, atti o dati coperti da segreto; usare esclusivamente i canali autorizzati dallo Studio e repository controllate (es. Lexroom per basi documentali legali, DeepL enterprise per traduzioni riservate, ecc.).

(e) Trasparenza verso i clienti.

Quando l'attività comporta l'uso di IA a supporto della prestazione, il cliente viene informato secondo quanto previsto dalla Legge 132/2025, art. 13, con linguaggio chiaro, semplice ed esaustivo.

(f) Contenuti sintetici.

Se si generano o manipolano contenuti suscettibili di essere percepiti come reali (immagini, audio, video, deepfake, ma anche testi che possono incidere sull'affidamento), si applicano gli obblighi di trasparenza/marcatura previsti dall'AI Act, art. 50.

Attività consentite/sconsigliate/vietate

(a) Sono consentite (con verifica):

- (i) ricerca giurisprudenziale/dottrinale;
- (ii) classificazione/riassunto di documenti;
- (iii) redazione di bozze e scalette;
- (iv) controllo stilistico/linguistico;
- (v) traduzioni di lavoro tramite canali enterprise;
- (vi) preparazione di presentazioni/strumenti interni.

(b) Sono sconsigliate senza autorizzazione del Capo Divisione:

- (i) caricamento massivo di fascicoli completi;
- (ii) analisi di dataset con dati personali particolari;
- (iii) benchmarking di strategie processuali su casi vivi;
- (iv) uso di modelli non autorizzati.

In tali casi si valuta DPIA/valutazione del rischio.

(c) Sono vietate:

- (i) decisioni automatizzate rivolte al cliente;
- (ii) profilazioni sensibili;
- (iii) riconoscimento emotivo o categorizzazione biometrica;
- (iv) caricamento di segreti professionali in servizi non enterprise;
- (v) generazione di contenuti sintetici realistici senza adeguata trasparenza/etichettatura.

Ruoli e responsabilità

- (a) **Capo Divisione / Referente IA di Divisione:** assegna gli accessi; autorizza i casi d'uso; verifica la corretta configurazione privacy; approva attività “*sensitive*”.
- (b) **Professionista incaricato:** valuta idoneità dello strumento al singolo incarico; prepara prompt minimizzati; verifica e valida l'output; documenta nel fascicolo l'uso dell'IA (nota interna sintetica su gestionale).
- (c) **IT/Compliance/DPO:** mantiene l'inventario strumenti e dei flussi dati; cura le impostazioni privacy; riesamina trimestralmente log, impostazioni e aggiornamenti contrattuali dei *vendor*.

Formazione e AI literacy

Lexant si impegna ad organizzare un programma iniziale di alfabetizzazione IA e aggiornamenti periodici, in adempimento dell'art. 4 AI Act. Modulo base (4 ore) su:

- (i) quadro normativo (AI Act, Legge 132/2025, GDPR);
- (ii) rischi tipici (bias, leakage, hallucinations);
- (iii) buone pratiche di prompt e data-minimization, policy dello Studio;
- (iv) moduli avanzati per Divisione;
- (v) verifica dell'apprendimento e attestato.

Il programma è documentato e aggiornato con cadenza semestrale.

Tracciabilità e audit

Per finalità difensive e di *accountability* si conserva, nel fascicolo interno (onedrive) e nel gestionale di Studio, un appunto sintetico che indichi lo strumento usato e le finalità. L'IT/Compliance effettua audit periodici e produce report ai Partner.

Data protection e trasferimenti

Lo Studio tratta i dati nel rispetto del GDPR; i fornitori autorizzati operano come responsabili del trattamento ove applicabile, con accordi art. 28 GDPR e, se fuori SEE, con adeguate garanzie (es. SCC). Per DeepL, Lexroom e Gamma si fa riferimento a documentazione di sicurezza e privacy resa pubblica dai fornitori; per OpenAI si applicano le condizioni business/enterprise, verificando le impostazioni che escludono l'uso per training. Tali elementi sono riesaminati annualmente.

Gestione incidenti

Qualsiasi anomalia (es. diffusione non autorizzata di output, riscontro di *bias*, risposte fuorvianti) è immediatamente segnalata al Capo Divisione e al DPO di Lexant; si sospende l'uso, si analizzano cause e si adotta rimedio correttivo; se coinvolti dati personali, si seguono le procedure *data-breach*.

Revisione

La presente policy è riesaminata almeno ogni 12 mesi o prima in caso di modifiche normative o tecniche rilevanti.