Valid from	15/08/2026	Jurisdiction	Italy / EU

Politica di Uso Accettabile

Piattaforma IndustryUX — Allegato incorporato per rinvio nelle Condizioni Generali di Abbonamento e Licenza

Codice documento	IUX-IT-35
Versione	1.2
Data	2026-08-11
Set	ANNEXES (IT)
Destinatari	Tutti i Clienti, gli Utenti Autorizzati e i titolari di account (B2B e B2C)
Lingua	Italiano (traduzione di cortesia — prevale la versione inglese)
Classificazione	Policy

Avviso — traduzione di cortesia. Questo documento è la traduzione italiana di cortesia del documento inglese IUX-EN-35, che è l'unica versione facente fede. In caso di divergenza fra le due versioni prevale, per ogni fine, la versione inglese.

Art. 1 — Finalità e oggetto

1.1 Finalità

La presente Politica di Uso Accettabile (la «Politica») definisce il perimetro dell'uso consentito della piattaforma IndustryUX, delle Applicazioni e di ogni servizio, interfaccia e deliverable messo a disposizione da DEVIBRAIN S.R.L., società di diritto italiano, con sede legale in Via Coghetti 6, 24128 Bergamo (BG), Italia, partita IVA e codice fiscale IT04507220160, posta elettronica certificata devibrain@pec.it (il «Fornitore (DevIBrain)», indicato nel resto della presente Politica come il «Fornitore»). Essa ha lo scopo di tutelare l'integrità, la sicurezza, la disponibilità e la liceità di una piattaforma industriale condivisa e multi-tenant, i diritti del Fornitore e dei terzi e la qualità del servizio erogato a tutti i clienti.

1.2 Natura della presente Politica

La presente Politica è un documento autonomo, incorporato per rinvio nella documentazione contrattuale e aggiornato conformemente all'Articolo 29 senza necessità di rinegoziare il Contratto.

Essa enuncia regole operative di condotta; non crea diritti commerciali, non modifica i corrispettivi e non estende né riduce i diritti di licenza concessi in forza del Contratto.

1.3 Ambito di applicazione

La presente Politica si applica a ogni canale commerciale e a ogni modello di deployment della piattaforma, inclusi gli acquisti self-service nello shop online, i piani Trial e Base, il piano Business, Enterprise Online, i deployment su server privato virtuale dedicato e le installazioni On-Premise, in quest'ultimo caso con riguardo alle componenti di licenza, attivazione, aggiornamento, supporto e verifica da remoto che continuano a interagire con l'infrastruttura del Fornitore.

Art. 2 — Soggetti vincolati e definizioni

2.1 Soggetti vincolati

La presente Politica vincola il Cliente e ogni soggetto che accede o utilizza la piattaforma attraverso l'account o gli Entitlement (titoli di licenza) del Cliente, inclusi gli Utenti Autorizzati, gli amministratori, i dipendenti, gli appaltatori, gli agenti, le società del gruppo del Cliente e ogni processo automatizzato, integrazione, script o applicazione di terzi che operi con le credenziali o le chiavi del Cliente. Il Cliente fa sì che tutti tali soggetti rispettino la presente Politica e resta responsabile verso il Fornitore della loro condotta, nei limiti dell'Articolo 13.

2.2 Definizioni

I termini definiti nelle Condizioni Generali di Abbonamento e Licenza (IUX-IT-01) hanno il medesimo significato nella presente Politica. In aggiunta:

Termine	Significato nella presente Politica
Contratto	le Condizioni Generali di Abbonamento e Licenza, le condizioni integrative di canale applicabili (le Condizioni Integrative Shop, Allegato A di canale, «Shop Schedule», IUX-IT-10, ovvero le Condizioni Integrative Enterprise, Allegato B, «Enterprise Schedule», IUX-IT-20), l'Ordine e tutti gli allegati, inclusa la presente Politica
Applicazioni	le applicazioni della piattaforma concesse in licenza al Cliente, come identificate nelle Condizioni Generali di Abbonamento e Licenza e nell'Ordine
Utente Autorizzato	la persona fisica autorizzata dal Cliente ad accedere alla piattaforma mediante credenziali individuali

Termine	Significato nella presente Politica
Dati del Cliente	ha il significato attribuito nelle Condizioni Generali di Abbonamento e Licenza e comprende tutti i dati, i file, i documenti, i disegni, i modelli tridimensionali, le immagini, i testi, le configurazioni, le ricette, il codice e gli altri materiali caricati sulla, memorizzati nella, trattati dalla o generati attraverso la piattaforma dal Cliente o da un Utente Autorizzato
Entitlement	il diritto d'uso contrattuale concesso al Cliente in forza del Contratto, come definito nelle Condizioni Generali di Abbonamento e Licenza, incluso il numero consentito di Utenti Autorizzati, attivazioni, Beni Designati e Applicazioni Generate e le dotazioni a consumo
Applicazione Generata	ciascun output prodotto attraverso le Applicazioni e vincolato a un Bene Designato, inclusi i controlli web esportati per i runtime di supervisione e di interfaccia uomo-macchina
Grant (record di licenza firmato)	la rappresentazione tecnica di un Entitlement, come definita nelle Condizioni Generali di Abbonamento e Licenza: il record firmato crittograficamente (ECDSA P-256) emesso dalla Console del Fornitore e registrato nel License Manager, che attesta i diritti d'uso, le dotazioni a consumo e il Bene Designato vincolato
Abuso Grave	ogni condotta elencata nell'Articolo 23
Token	l'unità di consumo prepagata che misura l'uso delle funzionalità a consumo, allocata a un Bene Designato e vincolata in via permanente ad esso, utilizzabile per qualsiasi consumo relativo al medesimo Bene Designato e non trasferibile ad altro; nei piani self-service disciplinati dallo Shop Schedule (Allegato A, IUX-IT-10) le corrispondenti unità sono accreditate nel wallet dell'account come Crediti Prepagati, non sono allocate ad alcun Bene Designato e seguono il regime di tale Allegato

Art. 3 — Rapporto con il Contratto e ordine di prevalenza

3.1 Incorporazione per rinvio

La presente Politica costituisce parte integrante e sostanziale del Contratto. L'accettazione del Contratto, in qualunque forma prevista per il canale di riferimento, costituisce accettazione della presente Politica. A ciascun atto di utilizzo si applica la versione in vigore al momento dell'atto medesimo.

3.2 Ordine di prevalenza

In caso di conflitto tra i documenti che compongono il Contratto, l'ordine di prevalenza è quello stabilito dall'Articolo 2.3 delle Condizioni Generali di Abbonamento e Licenza (IUX-IT-01), che si applica come tale e non è qui ripetuto. Ai fini di tale ordine la presente Politica si colloca tra gli altri allegati.

3.3 Violazione della presente Politica

La violazione della presente Politica costituisce inadempimento del Contratto. Conformemente all'Articolo 8.4 delle Condizioni Generali di Abbonamento e Licenza, le violazioni delle regole d'uso sono trattate mediante la procedura graduata di cui agli Articoli da 22 a 24 della presente Politica, e i rimedi per inadempimento grave previsti da tali Condizioni, inclusa la risoluzione ai sensi dell'art. 1456 c.c., sono riservati ai casi di Abuso Grave. In funzione della sua gravità la violazione legittima pertanto il Fornitore ad applicare tali misure graduate e, nei casi di Abuso Grave, a sospendere il servizio con effetto immediato e a risolvere il Contratto, fermi restando il risarcimento del danno e ogni altro rimedio previsto dalla legge.

Art. 4 — Principio generale di uso lecito e professionale

Il Cliente utilizza la piattaforma nel rispetto della legge, della presente Politica, del Contratto e della documentazione tecnica, per le proprie finalità professionali interne, in modo da non arrecare pregiudizio al Fornitore, agli altri clienti, agli Utenti Autorizzati o ai terzi. La piattaforma è uno strumento professionale di ingegneria industriale: non è destinata all'uso personale o domestico dei consumatori al di là dell'uso di valutazione e apprendimento espressamente consentito per i piani Trial e Base, e non è destinata all'uso da parte di minori.

Art. 5 — Usi vietati: attività illecite

Il Cliente e i suoi Utenti Autorizzati non utilizzano la piattaforma, direttamente o indirettamente, al fine di:

• commettere, preparare, agevolare od occultare qualsiasi reato o altro atto illecito, inclusi la frode, il riciclaggio, la corruzione, gli abusi di mercato, i reati tributari e i reati informatici;

• violare la normativa applicabile in materia industriale, ambientale, di sicurezza dei prodotti, di lavoro o di controllo a distanza dei lavoratori, incluso qualsiasi monitoraggio occulto dei dipendenti vietato dalla legge 300/1970 e dalla normativa in materia di protezione dei dati;

• svolgere attività soggette ad autorizzazione senza disporre dell'autorizzazione richiesta;

• violare le norme in materia di controllo delle esportazioni, embargo o sanzioni, come ulteriormente specificato nell'Articolo 20;

• violare i diritti dei terzi, inclusi i diritti della personalità, la riservatezza, i segreti commerciali e i diritti di proprietà intellettuale.

Art. 6 — Usi vietati: proprietà intellettuale e diritti dei terzi

Il Cliente e i suoi Utenti Autorizzati non possono:

• copiare, riprodurre, distribuire, vendere, locare, dare in prestito, concedere in sublicenza, pubblicare o comunque mettere a disposizione di terzi la piattaforma, le Applicazioni o le loro componenti al di fuori dei limiti del Contratto;

• rimuovere, alterare, occultare o falsificare marchi, loghi, avvisi di copyright, identificativi di licenza, indicazioni di versione o informazioni di provenienza apposti dal Fornitore alla piattaforma o alle Applicazioni Generate;

• caricare, trattare o distribuire attraverso la piattaforma materiale che violi il diritto d'autore, i brevetti, i marchi, i disegni e modelli, i segreti commerciali o i diritti sulle banche dati di terzi;

• utilizzare la piattaforma, la documentazione o le Applicazioni Generate per sviluppare, addestrare, commercializzare o supportare un prodotto o un servizio concorrente della piattaforma, ovvero per svolgere attività di benchmarking i cui risultati siano divulgati a terzi senza il previo consenso scritto del Fornitore;

• estrarre, replicare o riutilizzare, con mezzi automatizzati o altrimenti, la struttura, le interfacce, le librerie di componenti, i template o la documentazione della piattaforma oltre l'uso consentito dal Contratto.

Art. 7 — Usi vietati: integrità della licenza, Entitlement e misurazione dei consumi

7.1 Elusione delle misure tecniche di protezione

Il Cliente e i suoi Utenti Autorizzati non possono eludere, manomettere, disabilitare, emulare, replicare, contraffare o comunque interferire con i meccanismi di attivazione, autenticazione, verifica della firma, validazione dei Grant, misurazione dei consumi e controllo dell'uso della piattaforma, inclusi i Grant, i codici di attivazione, i file di licenza, il periodo di tolleranza offline, il conteggio dei Token e l'associazione di un'Applicazione Generata al relativo Bene Designato.

7.2 Uso eccedente gli Entitlement

Il Cliente e i suoi Utenti Autorizzati non possono utilizzare la piattaforma oltre i limiti degli Entitlement, in particolare eccedendo il numero di Utenti Autorizzati, attivazioni, Beni Designati, siti o Applicazioni Generate, condividendo credenziali individuali, utilizzando un unico account per più di una persona fisica, ovvero utilizzando un Grant emesso per un Bene Designato su una macchina o un impianto diversi. La sostituzione dell'hardware di controllo della medesima macchina, con l'identificativo aggiornato in Console conformemente all'Enterprise Schedule (Allegato B, IUX-IT-20), non costituisce uso su una macchina diversa e non integra violazione del presente Articolo.

7.3 Service bureau e fornitura a terzi

Il Cliente e i suoi Utenti Autorizzati non possono utilizzare la piattaforma per fornire servizi a terzi in forma di service bureau, outsourcing, time-sharing, hosting per conto di terzi o qualsiasi assetto equivalente, né consentire l'accesso a soggetti diversi dagli Utenti Autorizzati, salvo che un accordo di partner o rivenditore espressamente sottoscritto dal Fornitore lo consenta.

7.4 Reverse engineering ed eccezioni legali inderogabili

Il Cliente e i suoi Utenti Autorizzati non possono decompilare, disassemblare, sottoporre a reverse engineering o altrimenti tentare di ricavare il codice sorgente, la struttura, gli algoritmi o i meccanismi di protezione della piattaforma, delle Applicazioni o delle Applicazioni Generate. Tale divieto non si applica, e non deve essere interpretato come applicabile, agli atti che non possono essere legittimamente vietati in forza di norme inderogabili e, in particolare, alla decompilazione a fini di interoperabilità consentita dall'art. 6 della Direttiva 2009/24/CE e dall'art. 64-quater della legge 633/1941, che resta consentita alle condizioni ivi previste. Al fine di rendere non necessari tali atti, il Fornitore si impegna a fornire, su richiesta scritta motivata e a condizioni ragionevoli, le informazioni di interoperabilità necessarie affinché i programmi creati autonomamente dal Cliente possano interoperare con la piattaforma.

7.5 Valore probatorio

I registri di emissione, validazione e revoca dei Grant tenuti dalla Console e dal License Manager, unitamente ai registri di misurazione dei consumi, costituiscono prova degli Entitlement concessi e dell'uso fatto della piattaforma, salva prova contraria fornita dal Cliente.

Art. 8 — Usi vietati: abuso di messaggistica, rete e sistemi

Il Cliente e i suoi Utenti Autorizzati non possono:

• inviare, o utilizzare la piattaforma o le sue funzionalità di notifica, condivisione, invito e posta elettronica per inviare, comunicazioni commerciali non sollecitate, messaggi a catena o qualsiasi altra forma di spam, né utilizzare elenchi di indirizzi raccolti senza una valida base giuridica;

• introdurre, ospitare, trasmettere o distribuire malware, virus, ransomware, bombe logiche, backdoor, exploit kit o qualsiasi altro codice dannoso, ovvero credenziali, chiavi o dati ottenuti illecitamente;

• tentare di ottenere accesso non autorizzato alla piattaforma, alla sua infrastruttura, agli ambienti di altri tenant, ad account, chiavi o dati non propri, ovvero di elevare i privilegi oltre quelli concessi;

• interferire con il funzionamento della piattaforma, anche mediante attacchi di denial-of-service, flooding di traffico, saturazione deliberata di code, risorse o storage, o tentativi di aggirare il rate limiting, le quote o i meccanismi di isolamento;

• effettuare estrazioni massive automatizzate di dati, scraping sistematico, crawling o enumerazione massiva di interfacce o identificativi, al di fuori delle interfacce di programmazione applicativa documentate e dei limiti di cui all'Articolo 18;

• utilizzare le risorse della piattaforma per finalità estranee alle Applicazioni, inclusi il mining di criptovalute, il calcolo distribuito, l'hosting generico di file, il proxying, il relaying, il tunnelling o l'anonimizzazione di traffico di terzi;

• falsificare identificativi, intestazioni, indirizzi di rete, marcature temporali o log, o comunque occultare l'origine di qualsiasi attività svolta sulla piattaforma.

Art. 9 — Test di sicurezza e divulgazione coordinata delle vulnerabilità

9.1 Autorizzazione preventiva

I penetration test, le scansioni di vulnerabilità, gli stress test, i test di carico, le attività di red-teaming e ogni altro test di sicurezza della piattaforma, delle sue interfacce o dell'infrastruttura richiedono la previa autorizzazione scritta del Fornitore, che ne definisce l'ambito, l'ambiente, la finestra temporale e i punti di contatto. I test svolti senza tale autorizzazione costituiscono Abuso Grave ai sensi dell'Articolo 23.

9.2 Segnalazione delle vulnerabilità

Ogni vulnerabilità, difetto di sicurezza o comportamento anomalo individuato in buona fede, anche se rilevato accidentalmente, è segnalato senza ingiustificato ritardo a support@devibrain.com, con i dettagli tecnici necessari alla riproduzione, e non è divulgato a terzi né reso pubblico prima del momento anteriore tra la rimediazione della vulnerabilità e la scadenza di novanta giorni dalla segnalazione, salvo che un termine più breve sia richiesto dalla legge o concordato per iscritto tra le Parti.

9.3 Ricerca in buona fede

Il Fornitore non promuoverà azioni contrattuali nei confronti di chi segnali una vulnerabilità qualora tale soggetto abbia agito in buona fede, non abbia acceduto, copiato, alterato o esfiltrato dati oltre il minimo necessario a dimostrare la vulnerabilità, non abbia acceduto a dati personali di terzi, non abbia degradato il servizio, non abbia utilizzato la scoperta per altre finalità e abbia rispettato l'Articolo 9.2. La presente disposizione non limita i diritti dei terzi né gli effetti delle norme penali inderogabili.

9.4 Cooperazione regolamentare

Le Parti danno atto che il Fornitore può essere soggetto a obblighi di notifica relativi a vulnerabilità attivamente sfruttate e a incidenti gravi ai sensi del Regolamento (UE) 2024/2847, e che il Cliente può essere soggetto a obblighi di notifica di incidenti ai sensi del d.lgs. 138/2024. Ciascuna Parte

coopera in buona fede e fornisce le informazioni ragionevolmente necessarie affinché l'altra Parte possa adempiere a tali obblighi entro i termini applicabili.

Art. 10 — Sicurezza dell'account e gestione delle credenziali

10.1 Obblighi del Cliente

Il Cliente: mantiene riservate le credenziali e ne impedisce la condivisione; abilita l'autenticazione a più fattori per ogni account dotato di privilegi amministrativi, ove la piattaforma la renda disponibile; assegna a ciascun Utente Autorizzato i soli privilegi necessari al ruolo ricoperto; revoca tempestivamente l'accesso quando un Utente Autorizzato lascia l'organizzazione o cambia ruolo; mantiene accurati e aggiornati l'elenco degli Utenti Autorizzati e i recapiti amministrativi.

10.2 Dispositivi e postazioni di lavoro

Il Cliente utilizza la piattaforma da dispositivi protetti da misure di sicurezza ragionevoli e aggiornate e non memorizza credenziali o file di Grant in chiaro su dispositivi condivisi, in repository non protetti o in posizioni accessibili al pubblico.

10.3 Misure del Fornitore

Il Fornitore applica le misure tecniche e organizzative descritte nell'Articolo 28 dell'Enterprise Schedule (Allegato B, IUX-IT-20) e nell'Allegato 2 all'Accordo sul Trattamento dei Dati (IUX-IT-31), e può richiedere la reimpostazione delle credenziali, la revoca delle chiavi o la ri-verifica di un account ove sussistano ragionevoli motivi per ritenere che la sua sicurezza sia stata compromessa.

Art. 11 — Chiavi delle interfacce di programmazione applicativa, credenziali macchina e integrazioni

11.1 Protezione delle chiavi

Le chiavi delle interfacce di programmazione applicativa, gli account di servizio, le credenziali macchina, i codici di attivazione e i file di Grant sono emessi per il tenant del Cliente, sono personali di quest'ultimo e non sono trasferibili. Il Cliente li conserva in un secret manager o in un archivio protetto equivalente e non li incorpora nelle Applicazioni Generate, nei controlli web distribuiti a terzi, nel codice lato client, in repository di codice pubblici o condivisi, nei ticket di supporto, nella posta elettronica o nella documentazione.

11.2 Rotazione e revoca

Il Cliente ruota le chiavi almeno ogni dodici mesi e immediatamente in caso di sospetta compromissione, alla cessazione del rapporto con un soggetto che vi aveva accesso o su richiesta motivata del Fornitore. Il Fornitore può revocare una chiave con effetto immediato in presenza di evidenze di compromissione o abuso, informandone il Cliente ai sensi dell'Articolo 12.3.

11.3 Integrazioni e automazione

Le integrazioni, gli script, gli agent e le applicazioni di terzi che operano con le credenziali o le chiavi del Cliente rispettano la presente Politica, i limiti di frequenza documentati e gli standard di uso equo di cui all'Articolo 18. Il Cliente è responsabile della loro configurazione e del loro comportamento e disabilita tempestivamente ogni integrazione che generi traffico anomalo, chiamate duplicate o cicli di ritentativo incontrollati.

Art. 12 — Notifica di compromissione e cooperazione

12.1 Notifica da parte del Cliente

Il Cliente notifica al Fornitore senza ingiustificato ritardo e comunque entro ventiquattro ore dalla conoscenza qualsiasi compromissione, effettiva o sospetta, di credenziali, chiavi, Grant, account o ambienti connessi alla piattaforma, nonché qualsiasi uso non autorizzato del servizio. La notifica è inviata a support@devibrain.com e, ove il Cliente intenda conferirle data certa, anche a devibrain@pec.it.

12.2 Contenuto della notifica e cooperazione

La notifica indica, nella misura in cui siano noti, la natura dell'evento, gli account, le chiavi e gli ambienti coinvolti, il momento in cui esso è iniziato ed è stato rilevato, le categorie di dati potenzialmente interessate e le misure di contenimento adottate. Il Cliente coopera in buona fede nelle attività di indagine e di contenimento e attua senza ritardo le misure di rimediazione ragionevolmente indicate dal Fornitore.

12.3 Notifica da parte del Fornitore

Qualora il Fornitore rilevi la compromissione di un account, di una chiave o di un Grant del Cliente, ne informa il Cliente senza ingiustificato ritardo tramite i contatti amministrativi registrati nell'account, indicando le misure adottate. Ove l'evento coinvolga dati personali, si applicano gli obblighi di notifica, i termini e i ruoli previsti dall'Accordo sul Trattamento dei Dati e dagli artt. 33 e 34 del Regolamento (UE) 2016/679.

Art. 13 — Responsabilità per l'attività svolta con l'account

13.1 Principio

Il Cliente è responsabile di tutte le attività svolte attraverso il proprio account, i propri Entitlement, le proprie chiavi e le proprie integrazioni, nonché del rispetto della presente Politica da parte dei propri Utenti Autorizzati e dei soggetti elencati nell'Articolo 2.1, come se tali attività fossero proprie.

13.2 Limiti del principio

La responsabilità di cui all'Articolo 13.1 non si estende alle attività che il Cliente provi essere imputabili a una falla di sicurezza della piattaforma di cui il Fornitore sia responsabile, a condotte del Fornitore o dei suoi subfornitori, ovvero ad accessi non autorizzati notificati conformemente all'Articolo 12.1, con riferimento al periodo successivo alla notifica. Il Fornitore coopera in ogni caso per individuare l'origine dell'evento.

13.3 Consumatori

Ove il Cliente sia un consumatore, la responsabilità per le attività svolte con l'account è limitata ai casi in cui il consumatore versi in colpa e non è posto a carico del consumatore alcun onere probatorio eccedente quanto consentito dalle norme inderogabili. Si applicano le disposizioni dell'Articolo 28.

Art. 14 — Dati del Cliente: contenuti vietati

Il Cliente e i suoi Utenti Autorizzati non possono caricare sulla, memorizzare nella, trattare nella, generare attraverso o distribuire per mezzo della piattaforma contenuti che:

• siano illeciti, o il cui possesso o la cui diffusione costituisca reato, incluso il materiale raffigurante abusi sessuali su minori, che il Fornitore rimuove e segnala alle autorità competenti senza preavviso;

• siano diffamatori, denigratori, minacciosi, molesti, discriminatori, ovvero istighino alla violenza o all'odio;

• violino i diritti di proprietà intellettuale, i segreti commerciali o le informazioni riservate di terzi, inclusi disegni tecnici, modelli, librerie, font, immagini e documentazione per i quali il Cliente non disponga di un sufficiente diritto d'uso;

• contengano dati personali di terzi che il Cliente non è legittimato a trattare, o che il Cliente tratta senza una valida base giuridica, senza che sia stata resa l'informativa prescritta dalla legge, o al di là delle finalità concordate con l'interessato;

• contengano, senza il previo accordo scritto del Fornitore, categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento (UE) 2016/679, dati relativi a condanne penali e reati ai sensi dell'art. 10 del medesimo Regolamento, o dati personali di minori;

• contengano codice dannoso, exploit funzionanti, credenziali o dati ottenuti illecitamente;

• contengano informazioni classificate per ragioni di sicurezza nazionale, o dati tecnici soggetti a controllo delle esportazioni, in assenza delle autorizzazioni richieste.

Art. 15 — Dati personali caricati sulla piattaforma

15.1 Ruoli e garanzie

Ove il Cliente carichi dati personali sulla piattaforma, il Cliente agisce in qualità di titolare del trattamento e il Fornitore in qualità di responsabile del trattamento, conformemente all'Accordo sul Trattamento dei Dati. Il Cliente garantisce di disporre di una valida base giuridica, di avere reso agli interessati l'informativa prescritta e che il trattamento affidato al Fornitore è lecito.

15.2 Minimizzazione dei dati

Il Cliente non carica dati personali non necessari al funzionamento delle Applicazioni. In particolare, i modelli tridimensionali, i grafici, le ricette, le configurazioni di allarme, i file multimediali e i documenti utilizzati per l'addestramento delle funzionalità di intelligenza artificiale sono, per quanto possibile, privi di dati personali, pseudonimizzati o aggregati.

15.3 Conseguenze

Il caricamento di dati personali in violazione del presente Articolo costituisce violazione della presente Politica e dell'Accordo sul Trattamento dei Dati. Il Fornitore può richiedere al Cliente la rimozione dei dati interessati e, ove la violazione sia grave o persista dopo la diffida di cui all'Articolo 24, può applicare le misure previste dall'Articolo 23.

Art. 16 — Funzionalità di intelligenza artificiale: uso accettabile e trasparenza

16.1 Ruoli ai sensi del Regolamento (UE) 2024/1689

Il Fornitore agisce in qualità di fornitore dei sistemi di intelligenza artificiale inclusi nella piattaforma, in particolare delle funzionalità di addestramento e dell'assistente conversazionale locale; il Cliente che li utilizza nel proprio contesto professionale agisce in qualità di deployer. Ciascuna Parte adempie agli obblighi connessi al proprio ruolo.

16.2 Trasparenza

Il Cliente e i suoi Utenti Autorizzati non possono disabilitare, rimuovere, occultare o alterare l'avviso che informa l'utente che l'interazione avviene con un sistema di intelligenza artificiale, né le marcature leggibili da macchina che identificano i contenuti generati o manipolati artificialmente, né presentare tali contenuti come di origine umana ove la legge ne imponga l'identificabilità.

16.3 Modifica sostanziale

Qualora il Cliente modifichi sostanzialmente un sistema di intelligenza artificiale della piattaforma, in particolare mediante ulteriore addestramento, modifiche strutturali della pipeline di retrieval o modifiche della sua finalità prevista, tali da alterarne il comportamento o il profilo di rischio, il Cliente può divenire esso stesso fornitore della versione modificata ai sensi dell'art. 25 del Regolamento (UE) 2024/1689. Il Cliente ne informa preventivamente per iscritto il Fornitore e assume i conseguenti obblighi.

16.4 Usi vietati

Il Cliente e i suoi Utenti Autorizzati non possono utilizzare le funzionalità di intelligenza artificiale della piattaforma per alcuna pratica vietata dall'art. 5 del Regolamento (UE) 2024/1689, incluse l'inferenza delle emozioni dei lavoratori sul luogo di lavoro al di fuori dei casi consentiti per motivi medici o di sicurezza, il punteggio sociale, le tecniche manipolative o di sfruttamento e la generazione di materiale illecito. Essi non possono tentare di eludere le misure di sicurezza o i filtri dei sistemi, né utilizzarli per generare contenuti che violino gli Articoli 5, 6 o 14 della presente Politica.

16.5 Dati di addestramento

Il Cliente garantisce di disporre dei diritti necessari all'utilizzo dei documenti e dei dati sottoposti per l'addestramento e che tale utilizzo non viola i diritti dei terzi. Gli output delle funzionalità di intelligenza artificiale costituiscono materiale di supporto alle decisioni: essi devono essere verificati da personale qualificato prima di ogni utilizzo operativo.

Art. 17 — Impiego industriale, sorveglianza umana e usi critici esclusi

17.1 Natura della piattaforma

La piattaforma, le Applicazioni e le Applicazioni Generate sono strumenti di visualizzazione, supervisione, documentazione e supporto alle decisioni. Non sono progettati, testati o certificati come funzioni strumentate di sicurezza, come componenti di sicurezza di macchine o impianti, o come dispositivi di protezione.

17.2 Usi esclusi

Il Cliente e i suoi Utenti Autorizzati non possono utilizzare la piattaforma, le Applicazioni Generate o gli output delle funzionalità di intelligenza artificiale come unico o autonomo mezzo per funzioni di arresto di emergenza, protezione delle persone, interblocchi di sicurezza funzionale, rilevazione di incendi o gas, applicazioni medicali o di sostegno vitale, controllo di installazioni nucleari, controllo del traffico aereo o ferroviario, o qualsiasi altra applicazione in cui un malfunzionamento possa causare direttamente la morte, lesioni personali, gravi danni ambientali o danni catastrofici a cose, salvo che il Fornitore abbia espressamente acconsentito per iscritto a tale uso e siano stati soddisfatti i relativi requisiti di certificazione.

17.3 Sorveglianza umana e validazione

Il Cliente assicura una sorveglianza umana proporzionata al rischio del processo interessato, valida ogni Applicazione Generata in un ambiente di test prima dell'uso in produzione, mantiene una procedura documentata di rollback e resta responsabile del rispetto della normativa e delle norme tecniche in materia di sicurezza delle macchine e di sicurezza funzionale applicabili al proprio impianto.

Art. 18 — Uso equo delle risorse condivise

18.1 Principio

La piattaforma è erogata su infrastruttura condivisa. Il consumo di risorse deve essere coerente con il normale uso professionale delle Applicazioni da parte del numero di Utenti Autorizzati e del piano indicati nell'Ordine e non deve degradare il servizio erogato agli altri clienti.

18.2 Standard di uso equo

Si applicano i seguenti standard, in aggiunta agli eventuali limiti espressi indicati nell'Ordine o nella documentazione tecnica:

Risorsa condivisa	Standard di uso equo	Misurazione	Misura applicabile in caso di eccedenza
Chiamate alle interfacce di programmazione applicativa e ai servizi di licenza	i limiti di frequenza pubblicati nella documentazione tecnica e, se superiori, quelli indicati nell'Ordine; in assenza di limite pubblicato, un consumo non superiore al triplo del consumo medio dei clienti del medesimo piano	periodo mobile di trenta giorni, per tenant e per chiave	comunicazione e rate limiting decorsi cinque giorni lavorativi; rate limiting protettivo immediato ove sia a rischio la stabilità della piattaforma
Banda in uscita ed esportazione di dati	volumi coerenti con l'uso professionale delle Applicazioni da parte degli Utenti Autorizzati indicati nell'Ordine	periodo mobile di trenta giorni	come sopra; le esportazioni effettuate a fini di recupero dei dati o di passaggio ad altro fornitore (switching) non sono mai limitate al di sotto della velocità necessaria a completare il recupero entro trenta giorni
Archiviazione dei Dati del Cliente e degli asset di progetto	la capacità indicata nell'Ordine, con una tolleranza del dieci per cento	mensile, al termine del periodo	comunicazione e offerta di capacità aggiuntiva; nessuna cancellazione dei Dati del Cliente prima che siano decorsi trenta giorni dalla comunicazione

Risorsa condivisa	Standard di uso equo	Misurazione	Misura applicabile in caso di eccedenza
Sessioni concorrenti, job di build e job di esportazione	una sessione concorrente per Utente Autorizzato; esecuzione in coda dei job di build e di esportazione	continua	accodamento e scheduling equo; nessuna limitazione permanente senza preavviso
Funzionalità a consumo	il saldo prepagato di Token allocato a ciascun Bene Designato e, nei piani self-service disciplinati dallo Shop Schedule (Allegato A, IUX-IT-10), il saldo di Crediti Prepagati del wallet dell'account	per transazione	le funzionalità a consumo si arrestano all'esaurimento del saldo interessato, conformemente alle Condizioni Generali di Abbonamento e Licenza; il saldo di un Bene Designato non è mai utilizzato per un altro
Richieste di supporto	volumi coerenti con il piano di supporto indicato nell'Ordine	periodo mobile di trenta giorni	assegnazione di priorità e, in caso di volumi abusivi ripetuti, diffida ai sensi dell'Articolo 24

18.3 Effetto sui livelli di servizio

Il rate limiting, l'accodamento o la limitazione applicati ai sensi del presente Articolo in conseguenza di un consumo eccedente imputabile al Cliente non costituiscono indisponibilità ai fini dell'Accordo sui Livelli di Servizio (IUX-IT-30) e non danno luogo a service credit.

18.4 Uso eccedente gli Entitlement

Il consumo eccedente gli Entitlement è regolarizzato conformemente alle Condizioni Generali di Abbonamento e Licenza, mediante pagamento dei corrispettivi dovuti per l'uso eccedente, ferme restando le misure di cui agli Articoli da 22 a 24 qualora l'eccedenza derivi dall'elusione dei meccanismi di misurazione dei consumi.

Art. 19 — Protezione multi-tenant e gestione del traffico

19.1 Misure protettive

Ove un'attività, anche lecita, metta a rischio la stabilità, la sicurezza o le prestazioni dell'infrastruttura condivisa o di un altro tenant, il Fornitore può applicare, con effetto immediato e nella misura minima necessaria, misure protettive quali il rate limiting, l'accodamento, l'isolamento temporaneo dell'ambiente interessato o la sospensione di una singola funzionalità.

19.2 Comunicazione e proporzionalità

Le misure protettive sono proporzionate, limitate nel tempo e revocate non appena la causa sia cessata. Il Fornitore informa il Cliente senza ingiustificato ritardo e comunque entro ventiquattro ore dalla loro applicazione, indicandone la ragione, l'ambito e la durata prevista, e coopera con il Cliente per individuare una configurazione stabile.

19.3 Divieto di interferenza

Il Cliente e i suoi Utenti Autorizzati non possono tentare di eludere le misure protettive, di distribuire il traffico tra più account, tenant, chiavi o indirizzi di rete al fine di aggirare i limiti, né di creare account o Trial in serie al fine di ottenere risorse o benefici eccedenti quelli previsti dall'Ordine.

Art. 20 — Controllo delle esportazioni, sanzioni e destinazioni soggette a restrizioni

Il Cliente non può utilizzare, esportare, riesportare, trasferire o mettere a disposizione la piattaforma, le Applicazioni, le Applicazioni Generate o la relativa documentazione tecnica in violazione del Regolamento (UE) 2021/821 e delle norme in materia di controllo delle esportazioni, embargo e misure restrittive dell'Unione europea, della Repubblica Italiana e di ogni altra giurisdizione applicabile; a favore di persone o entità soggette a misure restrittive; verso territori sottoposti a embargo; ovvero per usi finali militari o connessi alla proliferazione di armi di distruzione di massa. I Clienti stabiliti al di fuori dell'Unione europea che non siano stabiliti in un paese partner elencato nel pertinente allegato al Regolamento (UE) 833/2014 rispettano il divieto di riesportazione verso, o di uso nella, Federazione Russa e nella Repubblica di Bielorussia previsto dalle Condizioni Generali di Abbonamento e Licenza. Qualora una verifica sulle liste applicabili dia esito positivo, il Fornitore sospende il servizio con effetto immediato fino al chiarimento della posizione, e tale sospensione non costituisce inadempimento del Fornitore.

Art. 21 — Monitoraggio, telemetria e prova

21.1 Che cosa monitora il Fornitore

Il Fornitore non ispeziona abitualmente il contenuto dei Dati del Cliente. Al fine di erogare il servizio, di proteggerne la sicurezza e di verificare il rispetto degli Entitlement, il Fornitore tratta telemetria tecnica, log di accesso, registri di misurazione dei consumi, registri di emissione e validazione dei Grant e segnali automatizzati di rilevamento degli abusi, nel rispetto dei principi di necessità e proporzionalità.

21.2 Accesso ai Dati del Cliente

L'accesso al contenuto dei Dati del Cliente da parte del personale del Fornitore avviene soltanto ove strettamente necessario per rispondere a una richiesta di supporto formulata dal Cliente, per contenere un incidente di sicurezza, per adempiere a un ordine vincolante di un'autorità

competente o per prevenire un reato di cui il Fornitore venga a conoscenza. Ogni accesso è registrato, limitato al personale autorizzato e vincolato a obblighi di riservatezza, ed è comunicato al Cliente salvo che una disposizione di legge lo vieti.

21.3 Conservazione dei registri

I log di sicurezza e di rilevamento degli abusi sono conservati per dodici mesi. I registri delle decisioni di enforcement adottate ai sensi della presente Politica e i registri di accettazione della presente Politica, inclusi l'identificativo di versione e l'hash del testo accettato, sono conservati per dieci anni su supporto a prova di manomissione, a fini di prova e di difesa dei diritti.

21.4 Audit

Il diritto di audit e verifica, il relativo preavviso, la sua frequenza e la preferenza per lo svolgimento da remoto sono disciplinati dalle Condizioni Generali di Abbonamento e Licenza. La presente Politica non estende tale diritto.

Art. 22 — Enforcement: principi e misure graduate

22.1 Principi

Il Fornitore applica le misure previste dalla presente Politica in buona fede, in modo proporzionato, tenendo conto della gravità, della reiterazione e degli effetti della violazione, e scegliendo la misura meno invasiva idonea a proteggere la piattaforma, i terzi e gli altri clienti. Il mancato esercizio di un diritto in una determinata occasione non costituisce rinuncia allo stesso.

22.2 Misure graduate

Livello	Situazioni tipiche	Misura	Preavviso
Livello 1 — violazione lieve	prima eccedenza di uno standard di uso equo; autenticazione a più fattori non abilitata su un account amministrativo; chiave non ruotata entro il termine di cui all'Articolo 11.2; non conformità formale isolata	diffida scritta con richiesta di rimediare	preavviso scritto, con quindici giorni per rimediare
Livello 2 — violazione significativa	ripetizione di un evento di Livello 1 dopo una diffida; condivisione di credenziali individuali; uso a beneficio di terzi al di fuori dell'Ordine; uso eccedente gli Entitlement rilevato attraverso i registri di licenza	rate limiting, limitazione della funzionalità o del singolo utente interessato, addebito dei corrispettivi dovuti per l'uso eccedente	preavviso scritto di cinque giorni lavorativi, con quindici giorni per rimediare

Livello	Situazioni tipiche	Misura	Preavviso
Livello 3 — Abuso Grave	le condotte elencate nell'Articolo 23	sospensione immediata dell'account, del tenant o della funzionalità interessata; risoluzione del Contratto ove la violazione non sia rimediata o non sia rimediabile	comunicazione scritta senza ingiustificato ritardo e comunque entro ventiquattro ore dalla sospensione

Art. 23 — Sospensione immediata per Abuso Grave

23.1 Casi

Il Fornitore può sospendere l'accesso alla piattaforma, in tutto o in parte, con effetto immediato, quando abbia ragionevoli e documentati motivi per ritenere che sussista una delle seguenti situazioni:

• elusione, manomissione o contraffazione dei meccanismi di attivazione, autenticazione, Grant o misurazione dei consumi di cui all'Articolo 7.1;

• reverse engineering al di fuori delle eccezioni legali inderogabili di cui all'Articolo 7.4;

• intrusione, tentativo di accesso non autorizzato, distribuzione di codice dannoso o attacco contro la piattaforma, la sua infrastruttura o un altro tenant;

• test di sicurezza svolti senza l'autorizzazione richiesta dall'Articolo 9.1;

• contenuti illeciti ai sensi dell'Articolo 14, o contenuti la cui conservazione esponga il Fornitore a responsabilità;

• violazione delle norme in materia di controllo delle esportazioni o di sanzioni di cui all'Articolo 20, ovvero esito positivo di una verifica sulle liste applicabili;

• condotte che degradino in misura rilevante il servizio erogato agli altri clienti o che mettano a rischio dati personali;

• uso escluso dall'Articolo 17.2 che metta a rischio la sicurezza delle persone;

• mancato pagamento dei corrispettivi, nei casi e decorsi i termini previsti dalle Condizioni Generali di Abbonamento e Licenza e dalle condizioni di pagamento.

23.2 Ambito e durata della sospensione

La sospensione è limitata, per quanto tecnicamente possibile, all'account, all'ambiente o alla funzionalità interessati ed è mantenuta soltanto per il tempo in cui la causa persiste o per il tempo necessario a mettere in sicurezza la piattaforma. Il Fornitore informa il Cliente ai sensi dell'Articolo 22.2, indicando i fatti, la misura adottata e l'attività di rimediazione richiesta.

23.3 Risoluzione

Qualora l'Abuso Grave non sia rimediato entro quindici giorni dalla comunicazione, o non sia rimediabile, o sia reiterato dopo una sospensione, il Fornitore può risolvere il Contratto con effetto immediato mediante comunicazione scritta, fermi restando il risarcimento del danno e il rimborso dei corrispettivi dovuti per l'eventuale uso eccedente gli Entitlement.

Art. 24 — Diffida e termine per rimediare per le altre violazioni

Per le violazioni della presente Politica diverse dall'Abuso Grave, il Fornitore diffida il Cliente per iscritto, indicando la condotta contestata, la disposizione violata e l'attività di rimediazione richiesta, e concede al Cliente quindici giorni per rimediare alla violazione e per darne prova. Durante tale periodo il Fornitore può applicare le misure di Livello 1 e di Livello 2 di cui all'Articolo 22.2, ma non può sospendere il servizio. Qualora la rimediazione non intervenga entro tale termine, il Fornitore può sospendere il servizio e, ove la violazione persista per ulteriori quindici giorni, risolvere il Contratto conformemente alle Condizioni Generali di Abbonamento e Licenza.

Art. 25 — Contestazione di una misura e ripristino

25.1 Contestazione

Il Cliente può contestare una misura adottata ai sensi della presente Politica scrivendo a support@devibrain.com entro quindici giorni dalla comunicazione, esponendo le proprie ragioni ed eventuali elementi di prova. Il Fornitore fornisce una risposta motivata entro dieci giorni lavorativi dal ricevimento e revoca o riduce la misura qualora la contestazione risulti fondata.

25.2 Ripristino

Qualora il Cliente rimedi alla violazione e ne confermi per iscritto la rimediazione, il Fornitore verifica la rimediazione e ripristina il pieno accesso entro due giorni lavorativi dall'esito positivo della verifica. Ove la rimediazione richieda un'attività del Fornitore, questi la esegue con la diligenza prevista dall'Accordo sui Livelli di Servizio (IUX-IT-30).

25.3 Misura ingiustificata

Qualora risulti accertato che una sospensione o una limitazione non era giustificata, il Fornitore ripristina il servizio senza indugio, proroga la durata dell'abbonamento per un periodo pari a quello della misura e accredita i corrispettivi relativi al periodo di indisponibilità. Resta impregiudicato ogni

ulteriore rimedio spettante al Cliente per legge, nei limiti di responsabilità previsti dalle Condizioni Generali di Abbonamento e Licenza.

25.4 Escalation

Qualora la contestazione non venga risolta, si applicano i meccanismi di risoluzione delle controversie previsti dalle condizioni integrative di canale applicabili, incluse, per i consumatori, le informazioni sulla risoluzione alternativa delle controversie ivi riportate.

Art. 26 — Effetti della sospensione e della risoluzione su dati, Token e corrispettivi

26.1 Dati del Cliente

La sospensione non comporta la cancellazione dei Dati del Cliente. Salvo il caso in cui la conservazione di specifici contenuti sia illecita, il Cliente conserva, durante la sospensione e per trenta giorni dalla risoluzione, il diritto di recuperare i Dati del Cliente e i dati esportabili nei formati strutturati descritti nella documentazione tecnica, senza alcun onere di switching. I diritti di recupero, portabilità e switching previsti dal Regolamento (UE) 2023/2854 e i relativi termini non sono pregiudicati da alcuna misura adottata ai sensi della presente Politica.

26.2 Token e Crediti Prepagati

La sospensione non consuma, non riduce e non estingue alcun saldo prepagato. Alla risoluzione si applicano due regimi distinti, che la presente Politica non altera. I Crediti Prepagati accreditati nel wallet dell'account ai sensi dello Shop Schedule (Allegato A, IUX-IT-10) non sono soggetti a decadenza: il Cliente ottiene l'accredito o il rimborso della parte non consumata, conformemente a tale Allegato. I Token allocati a un Bene Designato ai sensi dell'Enterprise Schedule (Allegato B, IUX-IT-20) restano vincolati a tale Bene Designato, sono utilizzabili soltanto per consumi ad esso relativi e non sono trasferiti ad altro Bene Designato, convertiti in credito o rimborsati, salvi i diritti inderogabili conferiti dalla legge. Qualora la risoluzione consegua a un Abuso Grave imputabile al Cliente, il Fornitore può compensare con l'eventuale credito o rimborso dovuto ai sensi del presente Articolo i corrispettivi dovuti per l'uso eccedente gli Entitlement e ogni danno documentato, fornendo un prospetto analitico. Restano impregiudicate le disposizioni inderogabili a tutela dei consumatori.

26.3 Corrispettivi

Qualora la sospensione sia imputabile a un inadempimento del Cliente, i corrispettivi continuano a maturare per la durata della sospensione, poiché il servizio resta disponibile per il Cliente all'atto della rimediazione. Nessun corrispettivo è dovuto per il periodo di una misura ingiustificata, conformemente all'Articolo 25.3.

Art. 27 — Segnalazione degli abusi e contatti

27.1 Segnalazioni

Chiunque può segnalare una violazione della presente Politica, contenuti illeciti o un evento di sicurezza a support@devibrain.com. Il Fornitore conferma il ricevimento entro due giorni lavorativi e completa la propria valutazione entro dieci giorni lavorativi, salvo che la complessità della questione richieda un termine più lungo, del quale il segnalante è informato. Le segnalazioni relative a materiale raffigurante abusi sessuali su minori, o a un rischio imminente per la sicurezza delle persone, sono trattate immediatamente.

27.2 Recapiti

Le comunicazioni ordinarie relative alla presente Politica sono indirizzate a support@devibrain.com; le comunicazioni generali a info@devibrain.com; le comunicazioni formali, anche ai fini della data certa, a devibrain@pec.it o alla sede legale in Via Coghetti 6, 24128 Bergamo (BG), Italia. Le comunicazioni al Cliente sono indirizzate ai contatti amministrativi registrati nell'account e, ove sia adottata una misura ai sensi dell'Articolo 23, anche all'indirizzo di posta elettronica del titolare dell'account.

Art. 28 — Consumatori: proporzionalità e diritti inderogabili

28.1 Proporzionalità

Ove il Cliente sia un consumatore, le misure previste dalla presente Politica sono applicate con particolare riguardo alla proporzionalità: la sospensione è adottata soltanto nei casi di Abuso Grave elencati nell'Articolo 23.1, il preavviso è dato ogniqualvolta la protezione della piattaforma o dei terzi lo consenta e ogni limitazione è circoscritta alla funzionalità interessata.

28.2 Diritti inderogabili

Nulla nella presente Politica limita i diritti inderogabili dei consumatori, inclusi la garanzia legale di conformità del contenuto digitale e dei servizi digitali, il diritto di recesso, il diritto a non subire la decadenza integrale delle somme versate in anticipo senza una corrispondente controprestazione e la competenza del foro del luogo di residenza o di domicilio eletto del consumatore. Ogni clausola della presente Politica che producesse tale effetto è nulla nei confronti del consumatore e non pregiudica la restante parte della presente Politica.

28.3 Risoluzione alternativa delle controversie

Le informazioni sugli organismi di risoluzione alternativa delle controversie sono riportate nello Shop Schedule (Allegato A, IUX-IT-10). Non è fatto rinvio alla piattaforma europea di risoluzione delle controversie online, dismessa a seguito del Regolamento (UE) 2024/3228.

Art. 29 — Modifiche della presente Politica

29.1 Preavviso

Il Fornitore può modificare la presente Politica con un preavviso di trenta giorni, dato mediante posta elettronica ai contatti amministrativi registrati nell'account e mediante avviso all'interno della piattaforma. La comunicazione identifica la versione, la data di entrata in vigore e il contenuto delle modifiche, e dà accesso alla versione precedente.

29.2 Motivi legittimi

Le modifiche possono essere apportate soltanto per un motivo legittimo indicato nella comunicazione, ossia: mutamenti della legge applicabile o delle prescrizioni di un'autorità competente; esigenze di sicurezza o schemi di abuso di nuova identificazione; modifiche dell'architettura, dell'infrastruttura o delle funzionalità della piattaforma; correzione di errori o chiarimento del testo.

29.3 Diritto di risoluzione

Qualora una modifica sia sostanzialmente sfavorevole al Cliente, il Cliente può risolvere il Contratto, senza penalità e con effetto dalla data di entrata in vigore della modifica, mediante comunicazione scritta inviata entro trenta giorni dalla comunicazione della modifica, e ha diritto al rimborso dei corrispettivi versati per il periodo non utilizzato e al trattamento dei Token e dei Crediti Prepagati non utilizzati previsto dall'Articolo 26.2. I consumatori possono in ogni caso recedere senza costi entro il medesimo termine. I termini di preavviso e i diritti applicabili alle modifiche dei corrispettivi restano disciplinati dalle Condizioni Generali di Abbonamento e Licenza.

29.4 Modifiche immediate

Qualora una modifica sia imposta da una disposizione di legge con effetto immediato o sia necessaria per contrastare una minaccia imminente per la sicurezza, essa ha effetto immediato; il Fornitore ne dà comunicazione appena possibile e il diritto di risoluzione previsto dall'Articolo 29.3 si applica a decorrere dalla data di tale comunicazione.

29.5 Registrazioni

Ciascuna versione della presente Politica è identificata da codice documento e numero di versione. Il Fornitore conserva il testo di ciascuna versione, l'hash del testo accettato e le evidenze di accettazione conformemente all'Articolo 21.3.

Art. 30 — Legge applicabile, foro competente e approvazione specifica delle clausole onerose

30.1 Legge applicabile e foro competente

La presente Politica è regolata dalla legge italiana. Per i clienti professionali è competente in via esclusiva il Foro di Bergamo, e il Fornitore mantiene la facoltà, a propria esclusiva scelta, di ricorrere all'arbitrato previsto dalle Condizioni Generali di Abbonamento e Licenza nei confronti di controparti stabilite al di fuori dell'Unione europea, dello Spazio economico europeo e degli Stati aderenti alla Convenzione di Lugano, unitamente al diritto di richiedere provvedimenti cautelari e decreti ingiuntivi dinanzi a qualsiasi giudice competente. È espressamente esclusa la Convenzione delle Nazioni Unite sui contratti di compravendita internazionale di merci. Per i consumatori si applicano la competenza del foro del luogo di residenza o di domicilio eletto del consumatore e le altre tutele inderogabili di cui all'Articolo 28.

30.2 Approvazione specifica

Ai sensi degli artt. 1341 e 1342 c.c., il Cliente che non sia un consumatore approva specificamente le seguenti clausole della presente Politica: Articolo 7 (divieti relativi all'integrità della licenza, agli Entitlement e alla misurazione dei consumi, e valore probatorio dei registri di licenza); Articolo 13 (responsabilità per le attività svolte con l'account); Articolo 18 (standard di uso equo e loro effetto sui livelli di servizio); Articolo 19 (misure protettive con effetto immediato); Articolo 21 (monitoraggio, telemetria, conservazione dei registri e prova); Articolo 22 (misure graduate di enforcement); Articolo 23 (sospensione con effetto immediato e risoluzione per Abuso Grave); Articolo 24 (termini per la rimediazione e risoluzione); Articolo 26 (effetti della sospensione e della risoluzione su Token e corrispettivi); Articolo 29 (modifica unilaterale della presente Politica); Articolo 30.1 (legge applicabile, foro esclusivo, arbitrato opzionale ed esclusione della Convenzione).

30.3 Modalità di rilascio dell'approvazione specifica

Nei canali che operano con accettazione mediante password monouso via posta elettronica, l'approvazione specifica di cui all'Articolo 30.2 è rilasciata attraverso un passaggio di conferma separato, distinto dall'accettazione della Politica nel suo complesso, registrato nell'audit trail con marca temporale, indirizzo di rete, user agent, account, versione del documento e hash. Nel canale riservato ai clienti professionali dell'Unione europea, l'approvazione specifica è rilasciata mediante la seconda sottoscrizione apposta al presente documento con firma elettronica qualificata, conformemente ai blocchi firma che seguono.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

Il blocco di approvazione specifica che segue si applica esclusivamente ai clienti professionali; esso non produce alcun effetto nei confronti dei consumatori.

Ai sensi e per gli effetti degli artt. 1341 e 1342 c.c., il Cliente dichiara di avere letto e di approvare specificamente le clausole richiamate nel presente blocco.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

Stato della presente versione e nota di validazione. Il presente documento è la release candidate v1.2 della Politica di Uso Accettabile IndustryUX, prodotta il 10 agosto 2026 e aggiornata l'11 agosto 2026 sulla base della normativa in vigore a tali date. Esso riflette decisioni operative assunte da DEVIBRAIN S.R.L. e ricerche giuridiche svolte internamente; non costituisce consulenza legale e non sostituisce una valutazione professionale. Prima di essere adottato con clienti reali, pubblicato o allegato a contratti sottoscritti, il presente testo deve essere validato da un avvocato qualificato e, per quanto riguarda gli Articoli 12, 14, 15, 16 e 21, dal responsabile della protezione dei dati o da un professionista della protezione dei dati, con particolare attenzione ai punti espressamente segnalati come bisognosi di verifica specialistica: la classificazione ai fini del controllo delle esportazioni del modulo crittografico di licenza, la classificazione dei modelli di deployment ai sensi del Regolamento (UE) 2024/2847 e l'applicabilità delle restrizioni alla riesportazione al software fornito su base autonoma. Una volta validato, il numero di versione e la data di entrata in vigore devono essere confermati e il testo registrato nel sistema di accettazione conformemente all'Articolo 29.5.

Changelog

Versione	Data	Modifiche
1.0	2026-08-10	Prima release candidate della Politica di Uso Accettabile (IUX-IT-35)
1.1	2026-08-11	Decisioni di gate: Token vincolati alla Macchina, validità dei Crediti Prepagati di 24 mesi, modello di Canone di Servizio On-Premise
1.1	2026-08-11	Traduzione italiana di cortesia della versione inglese 1.1
1.2	2026-08-11	Matrice piani 2026-08-11: il piano Pro è ridenominato Business ed Enterprise Cloud è ridenominato Enterprise Online nell'ambito di applicazione

Versione	Data	Modifiche
1.2	2026-08-11	Traduzione italiana di cortesia della versione inglese 1.2

IUX-IT-35 · v1.2 · 2026-08-11 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.