Valid from	15/08/2026	Jurisdiction	EU — Regulation (EU) 2016/679, art. 28

Accordo sul Trattamento dei Dati Personali

Allegato alle Condizioni Generali di Abbonamento e Licenza IndustryUX — Articolo 28 GDPR

Codice documento	IUX-IT-31
Versione	1.2
Data	2026-08-11
Set	ANNEXES (IT)
Destinatari	Clienti che agiscono in qualità di titolari del trattamento — canali Shop, Business, Enterprise Online, VPS e On-Premise
Lingua	Italiano (traduzione di cortesia — prevale la versione inglese)
Classificazione	Contractual document
Note	Include gli Allegati da 1 a 5 (descrizione del trattamento, misure di sicurezza, sub-responsabili, clausole contrattuali tipo 2021/914, valutazione d'impatto sul trasferimento)

Avviso — traduzione di cortesia. Questo documento è la traduzione italiana di cortesia del documento inglese IUX-EN-31, che è l'unica versione facente fede. In caso di divergenza fra le due versioni prevale, per ogni fine, la versione inglese.

Il presente Accordo sul Trattamento dei Dati Personali (il "DPA") è concluso tra **DEVIBRAIN S.R.L.**, società costituita secondo il 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 in tutto il presente DPA come il "Fornitore" e, per quanto riguarda il suo ruolo tecnico ai sensi del GDPR, come il "Responsabile del trattamento"), e il cliente identificato nell'Ordine (il "Titolare del trattamento" o il "Cliente"), ciascuno una "Parte" e insieme le "Parti".

Il DPA è concluso ai sensi dell'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 (il "GDPR"). Esso costituisce parte integrante e sostanziale delle Condizioni Generali di Abbonamento e Licenza IndustryUX (le "Master Terms", IUX-IT-01), delle Condizioni Integrative di canale applicabili, vale a dire le Condizioni Integrative Shop (Allegato A di canale, "Shop Schedule", IUX-IT-10) o le Condizioni

Integrative Enterprise ("Enterprise Schedule", IUX-IT-20), e di ciascun Ordine emesso ai sensi delle stesse (insieme, il "Contratto"), e disciplina il trattamento dei dati personali effettuato dal Fornitore per conto del Cliente nella fornitura della piattaforma IndustryUX e delle sue applicazioni (la "Piattaforma").

Ove il Contratto sia accettato attraverso il flusso self-service, il presente DPA è accettato insieme alle Master Terms e la sua accettazione è registrata nell'evidenza di accettazione descritta nelle Master Terms. Ove il Contratto sia sottoscritto attraverso il flusso con firma, il presente DPA è firmato insieme alle Master Terms.

Art. 1 — Definizioni e interpretazione

1.1 Termini definiti altrove

I termini con iniziale maiuscola non definiti nel presente DPA hanno il significato loro attribuito nelle Master Terms. I termini "dati personali", "categorie particolari di dati personali", "trattamento", "titolare del trattamento", "responsabile del trattamento", "sub-responsabile", "interessato", "violazione dei dati personali", "autorità di controllo" e "paese terzo" hanno il significato loro attribuito dal GDPR.

1.2 Definizioni specifiche

• **"Dati Personali del Cliente"** indica i dati personali contenuti nei Dati del Cliente che il Fornitore tratta per conto del Cliente nella fornitura della Piattaforma, come descritto nell'Allegato 1.

• **"Normativa sulla Protezione dei Dati"** indica il GDPR, il decreto legislativo italiano 196/2003 come modificato dal decreto legislativo 101/2018, la direttiva 2002/58/CE come attuata in Italia e ogni altra disposizione in materia di protezione dei dati applicabile al trattamento descritto nell'Allegato 1, ivi compresi i provvedimenti delle autorità di controllo.

• **"SEE"** indica lo Spazio Economico Europeo.

• **"SCC"** indica le clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi stabilite nella decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021, come modificata o sostituita.

• **"Sub-responsabile"** indica qualsiasi terzo incaricato dal Fornitore che tratti Dati Personali del Cliente per conto del Cliente.

• **"Pagina dei Sub-responsabili"** indica la pagina pubblica all'indirizzo https://www.industryux.com/legal/sub-processors, che elenca i Sub-responsabili in essere e consente di iscriversi alle notifiche di modifica.

• **"TIA"** indica la valutazione d'impatto sul trasferimento descritta nell'Allegato 5.

• **"Dati di Utilizzo"** indica i dati tecnici, di verifica della licenza e di telemetria generati dal funzionamento della Piattaforma, come descritti nell'Articolo 2 e nell'Informativa sulla Privacy IndustryUX.

1.3 Interpretazione

I titoli hanno valore meramente di comodità. "Compreso" e "incluso" significano "compreso, a titolo esemplificativo e non esaustivo". I riferimenti a testi normativi si intendono fatti a tali testi come modificati, sostituiti o rifusi nel tempo. Gli Allegati da 1 a 5 costituiscono parte integrante del presente DPA. I termini espressi in giorni si intendono in giorni di calendario, salvo che sia espressamente indicato che si tratta di giorni lavorativi.

Art. 2 — Ambito di applicazione, ruoli delle Parti e doppia veste

2.1 Il Fornitore come responsabile del trattamento

Con riferimento ai Dati Personali del Cliente, il Cliente agisce come titolare del trattamento e il Fornitore agisce come responsabile del trattamento. Il Fornitore tratta i Dati Personali del Cliente esclusivamente per fornire, gestire, mantenere, mettere in sicurezza e supportare la Piattaforma in conformità al Contratto e alle istruzioni documentate del Cliente.

2.2 Il Fornitore come titolare autonomo

Il Fornitore agisce come titolare autonomo del trattamento, e il presente DPA non si applica, con riferimento a: (a) i dati di registrazione, di account, di contatto e di fatturazione del Cliente e dei suoi rappresentanti aziendali; (b) i Dati di Utilizzo e la telemetria di verifica della licenza trattati per finalità di conformità delle licenze, prevenzione delle frodi, sicurezza, pianificazione della capacità e miglioramento del prodotto, che il Fornitore tratta in forma pseudonimizzata ove tecnicamente possibile; (c) le evidenze di accettazione dei documenti contrattuali, conservate in forma a prova di manomissione per dieci anni; (d) i dati di navigazione, di cookie e di marketing raccolti sul sito web pubblico. Tali attività di trattamento sono disciplinate dall'Informativa sulla Privacy IndustryUX e dalla Cookie Policy, e la loro base giuridica è l'esecuzione del contratto, l'adempimento di obblighi di legge o il legittimo interesse del Fornitore, come indicato in tale Informativa sulla Privacy. Il presente Articolo risolve, in favore della trasparenza, la doppia veste del Fornitore e prevale, secondo l'ordine di prevalenza richiamato all'Articolo 3.1, su qualsiasi lettura contraria delle disposizioni sulla telemetria e sull'audit delle Master Terms.

2.3 Cliente che agisce come responsabile del trattamento per un terzo

Se il Cliente è a sua volta un responsabile del trattamento che agisce per conto di uno o più titolari terzi, il Fornitore agisce come sub-responsabile e il presente DPA si applica mutatis mutandis. Il Cliente garantisce di disporre delle autorizzazioni necessarie per incaricare il Fornitore e per

impartire le istruzioni previste dal presente DPA, e che il proprio accordo con il titolare terzo è coerente con il presente DPA.

2.4 Consumatori e canali self-service

Per i clienti che acquisiscono la Piattaforma attraverso il canale Shop per scopi esclusivamente personali o domestici si applica, al loro proprio utilizzo, l'esclusione di cui all'articolo 2, paragrafo 2, lettera c), del GDPR e il presente DPA non si applica; il Fornitore resta titolare dei dati descritti all'Articolo 2.2. Il presente DPA si applica ai Clienti Shop e Trial soltanto ove e nella misura in cui essi utilizzino la Piattaforma nell'esercizio di un'attività professionale e carichino dati personali relativi a terzi.

2.5 Garanzie del Cliente

Il Cliente garantisce che: (a) dispone di un'appropriata base giuridica per il trattamento che istruisce; (b) ha fornito agli interessati le informazioni richieste dagli articoli 13 e 14 del GDPR, non avendo il Fornitore alcun rapporto diretto con essi; (c) i Dati Personali del Cliente da esso caricati sono adeguati, pertinenti e limitati a quanto necessario; e (d) ha valutato l'idoneità delle misure di sicurezza della Piattaforma, descritte nell'Allegato 2, rispetto al rischio del proprio trattamento.

Art. 3 — Ordine di prevalenza

3.1 Gerarchia

L'ordine di prevalenza tra i documenti del Contratto, compreso il rango del presente DPA in materia di protezione dei dati, è l'unico ordine di prevalenza stabilito all'Articolo 2.3 delle Master Terms (IUX-IT-01); esso non è qui riprodotto e si applica al presente DPA come si applica a ogni altro documento del Contratto. Ove si applichino le SCC o qualsiasi altro strumento di trasferimento sottoscritto dalle Parti, essi prevalgono sul presente DPA in caso di conflitto, in conformità all'Articolo 11.3 e all'Allegato 4.

3.2 Norme imperative

Nessuna disposizione del presente DPA limita o esclude un obbligo che la Normativa sulla Protezione dei Dati impone a una delle Parti, né i diritti che gli interessati ne traggono. Qualsiasi disposizione che risulti incompatibile con la Normativa sulla Protezione dei Dati va letta come modificata nella misura minima necessaria a renderla compatibile, restando impregiudicata la parte rimanente.

Art. 4 — Oggetto, durata, natura e finalità del trattamento

4.1 Descrizione

L'oggetto, la durata, la natura e la finalità del trattamento, i tipi di dati personali, le categorie di interessati, la frequenza del trattamento e i periodi di conservazione sono descritti nell'Allegato 1, che soddisfa l'articolo 28, paragrafo 3, del GDPR e costituisce altresì l'Allegato I.B delle SCC ove le SCC si applichino.

4.2 Durata

Il trattamento ha la durata del Contratto e, successivamente, dei periodi di recupero e cancellazione stabiliti all'Articolo 14. Restano impregiudicati gli obblighi di conservazione di legge che riguardano il Fornitore in qualità di titolare ai sensi dell'Articolo 2.2.

4.3 Attivazione di ulteriori moduli

Se il Cliente attiva un modulo della Piattaforma non elencato nell'Allegato 1, l'Allegato 1 si intende integrato dalla descrizione di tale modulo pubblicata dal Fornitore e comunicata al Cliente al momento dell'attivazione, senza alcuna riduzione delle tutele del presente DPA.

Art. 5 — Istruzioni documentate

5.1 Trattamento solo su istruzione

Il Fornitore tratta i Dati Personali del Cliente soltanto su istruzioni documentate del Cliente, anche in relazione ai trasferimenti verso un paese terzo. Costituiscono istruzioni documentate: il Contratto e il presente DPA; l'Ordine; la configurazione, le opzioni e le impostazioni selezionate dal Cliente all'interno della Piattaforma; l'utilizzo delle funzioni della Piattaforma da parte del Cliente e dei suoi Utenti Autorizzati; e ogni ulteriore istruzione scritta impartita ai sensi dell'Articolo 5.2.

5.2 Ulteriori istruzioni

Le ulteriori istruzioni sono impartite per iscritto al punto di contatto indicato all'Articolo 19. Il Fornitore dà attuazione alle istruzioni compatibili con le funzioni della Piattaforma e con la Normativa sulla Protezione dei Dati. Ove un'istruzione richieda sviluppi, configurazioni o attività che eccedono le funzioni ordinarie della Piattaforma, il Fornitore ne informa preventivamente il Cliente e può subordinarne l'esecuzione al pagamento di un corrispettivo ragionevole basato sulle tariffe indicate nell'Ordine o, in mancanza di tali tariffe, sulle proprie tariffe standard per servizi professionali in vigore.

5.3 Istruzioni illegittime

Il Fornitore informa il Cliente senza ingiustificato ritardo se, a suo avviso, un'istruzione viola la Normativa sulla Protezione dei Dati, e può sospendere l'esecuzione di tale istruzione fino a che essa non sia confermata, modificata o ritirata per iscritto, senza che tale sospensione costituisca inadempimento del Fornitore. Il Fornitore non è tenuto a svolgere una valutazione giuridica delle istruzioni del Cliente.

5.4 Trattamento richiesto dalla legge

Se il diritto dell'Unione o dello Stato membro cui è soggetto il Fornitore gli impone di trattare i Dati Personali del Cliente diversamente dalle istruzioni del Cliente, il Fornitore informa il Cliente di tale obbligo giuridico prima del trattamento, salvo che tale diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

5.5 Nessun trattamento per finalità proprie

Il Fornitore non tratta i Dati Personali del Cliente per finalità proprie, non li vende, non li rende disponibili a terzi diversi dai Sub-responsabili elencati nell'Allegato 3 e non li utilizza per addestrare, mettere a punto o migliorare modelli o funzioni messi a disposizione di altri clienti, secondo quanto ulteriormente previsto all'Articolo 15.

5.6 Categorie particolari e minimizzazione

Il Cliente è istruito a non caricare sulla Piattaforma categorie particolari di dati personali ai sensi dell'articolo 9 del GDPR né dati relativi a condanne penali e reati ai sensi dell'articolo 10 del GDPR, salvo quanto espressamente concordato per iscritto nell'Ordine unitamente alle misure supplementari richieste dal rischio. La Piattaforma non è progettata per trattare tali dati in via ordinaria e il Fornitore non effettua alcun controllo preventivo sui contenuti caricati dal Cliente.

Art. 6 — Riservatezza e personale autorizzato

6.1 Impegni del personale

Il Fornitore assicura che le persone autorizzate a trattare i Dati Personali del Cliente si siano impegnate per iscritto alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza, abbiano ricevuto istruzioni e formazione periodica in materia di protezione dei dati e accedano ai Dati Personali del Cliente soltanto nella misura strettamente necessaria allo svolgimento delle proprie mansioni.

6.2 Gestione degli accessi

L'accesso agli ambienti di produzione è nominativo, individuale, soggetto ad autenticazione a più fattori, concesso secondo il principio del privilegio minimo e registrato. L'accesso di supporto a un tenant è concesso soltanto per il tempo necessario a gestire la richiesta ed è revocato alla chiusura della richiesta. I diritti di accesso sono riesaminati almeno ogni sei mesi e revocati lo stesso giorno in cui cessa il rapporto di lavoro o professionale.

6.3 Ultrattività

Gli obblighi di riservatezza sopravvivono alla cessazione del Contratto per tutto il tempo in cui le informazioni conservano carattere riservato e, in ogni caso, per cinque anni, ferma restando la protezione perpetua dei dati personali richiesta dalla Normativa sulla Protezione dei Dati.

Art. 7 — Sicurezza del trattamento

7.1 Misure tecniche e organizzative

Il Fornitore attua e mantiene le misure tecniche e organizzative descritte nell'Allegato 2, adeguate al rischio ai sensi dell'articolo 32 del GDPR tenuto conto dello stato dell'arte, dei costi di attuazione e della natura, dell'oggetto, del contesto e delle finalità del trattamento. L'Allegato 2 è contrattualmente vincolante e costituisce altresì l'Allegato II delle SCC ove le SCC si applichino.

7.2 Evoluzione delle misure

Il Fornitore può aggiornare le misure dell'Allegato 2 per stare al passo con l'evoluzione tecnica, purché il livello di sicurezza non sia sostanzialmente ridotto. Gli aggiornamenti sostanziali sono comunicati al Cliente almeno trenta giorni prima della loro efficacia.

7.3 Responsabilità del Cliente

Il Cliente è responsabile della corretta configurazione dei ruoli, dei permessi e delle opzioni messi a disposizione dalla Piattaforma, della gestione e custodia delle credenziali dei propri Utenti Autorizzati, della scelta dei contenuti che carica e, nel modello di deployment On-Premise, della sicurezza della propria rete, dei propri sistemi e dei propri locali. Il Fornitore non è responsabile delle conseguenze di configurazioni, permessi o caricamenti decisi dal Cliente, né della sicurezza di ambienti che il Fornitore non gestisce.

7.4 Cooperazione sulla sicurezza delle reti e sulla sicurezza dei prodotti

Le Parti cooperano in buona fede affinché ciascuna possa adempiere ai propri obblighi ai sensi della direttiva (UE) 2022/2555 (NIS2) come attuata in Italia dal decreto legislativo 138/2024 e, per i componenti qualificabili come prodotti con elementi digitali, ai sensi del regolamento (UE) 2024/2847 (Cyber Resilience Act), inclusa la segnalazione delle vulnerabilità attivamente sfruttate applicabile dall'11 settembre 2026. Il Fornitore informa il Cliente delle vulnerabilità che riguardano la Piattaforma e che richiedono un intervento del Cliente, unitamente alle mitigazioni disponibili. Un addendum sulla resilienza operativa digitale ai sensi del regolamento (UE) 2022/2554 (DORA) è reso disponibile su richiesta ai clienti soggetti a tale regolamento.

7.5 Certificazioni

Alla data della versione il Fornitore non è titolare di una certificazione ai sensi dell'articolo 42 del GDPR e non aderisce a un codice di condotta approvato ai sensi dell'articolo 40 del GDPR, e non rende alcuna dichiarazione in senso contrario. Il Fornitore mette a disposizione del Cliente la propria documentazione di sicurezza, le risposte al suo questionario di sicurezza e le evidenze descritte all'Articolo 13.

Art. 8 — Sub-responsabili

8.1 Autorizzazione generale

Il Cliente concede al Fornitore un'autorizzazione scritta generale a incaricare Sub-responsabili, ai sensi dell'articolo 28, paragrafo 2, del GDPR e della clausola 9, lettera a), Opzione 2, delle SCC, nel rispetto della procedura prevista dal presente Articolo.

8.2 Elenco in essere

I Sub-responsabili autorizzati alla data della versione sono elencati nell'Allegato 3. L'elenco aggiornato è pubblicato sulla Pagina dei Sub-responsabili, che consente al Cliente anche di iscriversi alle notifiche di modifica via posta elettronica. Il Cliente si impegna a mantenere iscritto a tali notifiche almeno un indirizzo di posta elettronica valido.

8.3 Preavviso delle modifiche

Il Fornitore comunica al Cliente l'intenzione di aggiungere o sostituire un Sub-responsabile almeno trenta giorni prima che tale Sub-responsabile inizi a trattare Dati Personali del Cliente. La comunicazione indica l'identità del Sub-responsabile, il servizio a esso affidato, il luogo del trattamento, le categorie di dati interessate e, per i trattamenti al di fuori del SEE, lo strumento di trasferimento utilizzato.

8.4 Opposizione e rimedi

Entro quindici giorni dalla comunicazione il Cliente può opporsi per iscritto per motivi ragionevoli attinenti alla protezione dei dati personali. Le Parti discutono quindi l'opposizione in buona fede per un ulteriore periodo di trenta giorni e il Fornitore propone, ove disponibile, una ragionevole soluzione alternativa. In mancanza di accordo entro tale termine, il Cliente può risolvere, senza penali e mediante comunicazione scritta, i servizi effettivamente interessati dalla modifica, con rimborso pro rata dei Corrispettivi pagati per il periodo non utilizzato e, quanto ai saldi prepagati, con il trattamento previsto dalle Master Terms e dalle Condizioni Integrative di canale applicabili: i Crediti Prepagati del wallet dell'account sono accreditati o rimborsati ai sensi dello Shop Schedule (IUX-IT-10), mentre i Token accreditati al wallet di una Macchina Designata restano vincolati a tale Macchina ai sensi dell'Enterprise Schedule (IUX-IT-20) e non sono convertiti in un credito né in un rimborso, salvi i diritti che la legge applicabile non consente di escludere. In pendenza della discussione, il Fornitore non affida i Dati Personali del Cliente opponente al nuovo Sub-responsabile, ove tecnicamente possibile.

8.5 Obblighi imposti ai Sub-responsabili e responsabilità

Il Fornitore impone a ciascun Sub-responsabile, mediante contratto scritto, obblighi di protezione dei dati almeno equivalenti a quelli del presente DPA, anche quanto a misure di sicurezza, riservatezza, assistenza, audit e trasferimenti internazionali. Il Fornitore resta pienamente responsabile nei confronti del Cliente dell'adempimento degli obblighi del Sub-responsabile ai sensi dell'articolo 28, paragrafo 4, del GDPR.

8.6 Sostituzione urgente

Ove un Sub-responsabile debba essere sostituito immediatamente per ragioni di sicurezza, di

continuità del servizio o a causa della sua insolvenza o non conformità, il Fornitore può procedere alla sostituzione e ne dà comunicazione al Cliente il prima possibile e comunque entro cinque giorni lavorativi, restando impregiudicati il diritto di opposizione del Cliente e i rimedi di cui all'Articolo 8.4.

Art. 9 — Assistenza per le richieste degli interessati

9.1 Funzioni messe a disposizione

Tenuto conto della natura del trattamento, il Fornitore assiste il Cliente mettendo a disposizione le funzioni della Piattaforma che consentono al Cliente di accedere, rettificare, cancellare, limitare, esportare e comunicare autonomamente i Dati Personali del Cliente, così da consentire al Cliente di rispondere alle richieste di cui agli articoli da 15 a 22 del GDPR.

9.2 Richieste ricevute direttamente

Se il Fornitore riceve una richiesta da un interessato relativa ai Dati Personali del Cliente, non vi risponde nel merito, informa il richiedente che la richiesta deve essere rivolta al Cliente ove ciò sia lecito, e trasmette la richiesta al Cliente senza ingiustificato ritardo e comunque entro cinque giorni lavorativi dal ricevimento.

9.3 Assistenza aggiuntiva

Ove il Cliente non possa soddisfare una richiesta attraverso le funzioni della Piattaforma, il Fornitore presta una ragionevole assistenza aggiuntiva. Tale assistenza è compresa nei Corrispettivi, salvo per le richieste manifestamente eccessive o ripetitive, che il Fornitore può addebitare alle tariffe indicate nell'Ordine o, in mancanza di tali tariffe, alle proprie tariffe standard per servizi professionali in vigore, previa comunicazione al Cliente del costo stimato.

Art. 10 — Incidenti di sicurezza, violazioni dei dati personali, valutazioni d'impatto

10.1 Notifica al Cliente

Il Fornitore notifica al Cliente qualsiasi violazione dei dati personali che riguardi i Dati Personali del Cliente senza ingiustificato ritardo e comunque entro quarantotto ore dal momento in cui ne viene a conoscenza. La conoscenza si ha quando il Fornitore dispone di un ragionevole grado di certezza che si sia verificato un incidente di sicurezza che ha determinato una violazione di dati personali.

10.2 Contenuto della notifica

La notifica contiene, nella misura in cui siano allora disponibili: la natura della violazione e, ove possibile, le categorie e il numero approssimativo di interessati e di record interessati; le probabili conseguenze; le misure adottate o proposte per porre rimedio alla violazione e attenuarne gli effetti; il punto di contatto per ulteriori informazioni. Ove le informazioni non siano immediatamente disponibili, esse sono fornite in fasi successive senza ulteriore ingiustificato ritardo.

10.3 Cooperazione e rimedi

Il Fornitore indaga sulla violazione, adotta le misure ragionevolmente necessarie per contenerla e porvi rimedio, conserva le evidenze e i log pertinenti e coopera con il Cliente affinché quest'ultimo possa adempiere ai propri obblighi ai sensi degli articoli 33 e 34 del GDPR. Il Fornitore non notifica all'autorità di controllo né agli interessati per conto del Cliente, salvo espressa istruzione scritta in tal senso.

10.4 Nessun riconoscimento

La notifica di una violazione e la cooperazione descritte nel presente Articolo non costituiscono alcun riconoscimento di colpa o di responsabilità da parte del Fornitore.

10.5 Valutazioni d'impatto e consultazione preventiva

Tenuto conto della natura del trattamento e delle informazioni a sua disposizione, il Fornitore assiste il Cliente nell'effettuazione delle valutazioni d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del GDPR e nella consultazione preventiva ai sensi dell'articolo 36 del GDPR, fornendo informazioni sull'architettura, sui flussi di dati, sui periodi di conservazione e sulle misure di sicurezza della Piattaforma. Il Cliente resta responsabile della valutazione e delle decisioni che assume sulla sua base.

Art. 11 — Localizzazione dei dati e trasferimenti internazionali

11.1 Localizzazione

I Dati Personali del Cliente trattati dal Fornitore nei modelli di deployment Business, Enterprise Online e VPS e nell'ambiente condiviso dei piani self-service dello shop sono ospitati all'interno del SEE, nel data centre primario gestito dal Fornitore in Italia e, per le copie di ridondanza, in strutture situate all'interno del SEE. Nel modello di deployment On-Premise i Dati Personali del Cliente restano sui sistemi del Cliente, come previsto all'Articolo 16.

11.2 Condizioni per i trasferimenti

Il Fornitore non trasferisce Dati Personali del Cliente al di fuori del SEE e non ne consente l'accesso dall'esterno del SEE, salvo che ricorra una delle seguenti condizioni: (a) è in vigore una decisione di adeguatezza della Commissione europea per il paese o per il destinatario; (b) sono state sottoscritte le SCC nel modulo applicabile al caso ed è stata completata con esito positivo la TIA descritta nell'Allegato 5, unitamente alle misure supplementari da essa individuate; oppure (c) si applica una deroga ai sensi dell'articolo 49 del GDPR su previa istruzione scritta del Cliente e sotto la sua responsabilità.

11.3 Clausole contrattuali tipo

Le SCC sono incorporate nel presente DPA per rinvio e sono completate secondo quanto stabilito nell'Allegato 4, che individua i moduli applicabili, le opzioni selezionate e la corrispondenza tra gli allegati delle SCC e gli allegati del presente DPA. Ove le SCC si applichino, esse prevalgono sul presente DPA in caso di conflitto.

11.4 EU-US Data Privacy Framework

Il Fornitore non fonda i trasferimenti in via primaria sulla decisione di adeguatezza del 10 luglio 2023 relativa all'EU-US Data Privacy Framework, per le ragioni esposte nell'Allegato 4, e adotta le SCC combinate con una TIA quale base primaria per i trasferimenti verso gli Stati Uniti. La certificazione di un importatore nell'ambito di tale framework, ove presente, è trattata come elemento aggiuntivo di valutazione e mai come sostituto delle SCC e della TIA.

11.5 Trasferimenti successivi

Il Fornitore assicura che ciascun Sub-responsabile stabilito al di fuori del SEE, o che renda i dati accessibili dall'esterno del SEE, sia vincolato dalle SCC nel modulo applicabile e dalle misure supplementari individuate nella TIA, e che ogni trasferimento successivo sia soggetto alle medesime condizioni.

11.6 Regno Unito e Svizzera

I trasferimenti verso il Regno Unito avvengono sulla base delle decisioni di adeguatezza rinnovate dalla Commissione europea il 19 dicembre 2025 e valide fino al 27 dicembre 2031; non è richiesto alcuno strumento di trasferimento aggiuntivo finché tali decisioni restano in vigore. Se nella catena viene introdotto un esportatore del Regno Unito, all'SCC si aggiunge l'addendum sui trasferimenti internazionali di dati emesso dall'Information Commissioner's Office. Per i trasferimenti soggetti alla legge federale svizzera sulla protezione dei dati, le SCC si applicano con gli adattamenti riconosciuti dall'Incaricato federale svizzero della protezione dei dati e della trasparenza.

Art. 12 — Richieste delle autorità pubbliche

12.1 Gestione delle richieste

Se il Fornitore o un Sub-responsabile riceve una richiesta giuridicamente vincolante da un'autorità pubblica, compresa un'autorità giudiziaria, di divulgazione di Dati Personali del Cliente, il Fornitore: (a) ne informa il Cliente senza ingiustificato ritardo, salvo che ciò sia vietato dalla legge, nel qual caso compie ogni sforzo ragionevole per ottenere una deroga al divieto e documenta tali sforzi; (b) contesta la richiesta ove sussistano ragionevoli motivi per ritenerla illegittima secondo il diritto del paese richiedente o secondo il diritto dell'Unione, anche mediante i mezzi di impugnazione e le misure cautelari disponibili; (c) divulga soltanto la quantità minima di dati legittimamente richiesta; (d) documenta la richiesta e la risposta e mette tale documentazione a disposizione del Cliente e, su richiesta, dell'autorità di controllo competente.

12.2 Nessun accesso diretto o illimitato

Il Fornitore non concede ad alcuna autorità pubblica un accesso diretto, illimitato o generalizzato ai Dati Personali del Cliente, non crea né mantiene back door o mezzi di accesso equivalenti e non è titolare di alcun obbligo di tale natura nei confronti di alcuna autorità pubblica. Il Fornitore informa prontamente il Cliente qualora non sia più in grado di rendere tale dichiarazione.

Art. 13 — Audit e dimostrazione della conformità

13.1 Informazioni

Il Fornitore mette a disposizione del Cliente tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dall'articolo 28 del GDPR, compresa la descrizione delle misure di sicurezza, il registro delle attività di trattamento tenuto ai sensi dell'articolo 30, paragrafo 2, del GDPR per la parte che riguarda il Cliente, e l'elenco dei Sub-responsabili.

13.2 Procedura di audit

Il Cliente può svolgere un audit con preavviso scritto di almeno trenta giorni, una volta ogni dodici mesi, in orario lavorativo, con modalità che non pregiudichino il funzionamento della Piattaforma. L'audit è condotto, in prima battuta, da remoto, mediante esame della documentazione, questionari e sessioni a distanza con il personale responsabile; un audit in loco presso la sede del Fornitore può essere svolto soltanto ove l'audit da remoto si sia rivelato oggettivamente insufficiente e le ragioni siano indicate per iscritto.

13.3 Auditor

Il Cliente può nominare un auditor terzo, purché questi non sia un concorrente del Fornitore e sia vincolato da obblighi di riservatezza almeno equivalenti a quelli del Contratto. Il Fornitore può opporsi, con motivazione, a uno specifico auditor, nel qual caso il Cliente ne nomina un altro.

13.4 Costi

Ciascuna Parte sostiene i propri costi dell'audit; il costo delle risorse che il Fornitore dedica all'audit oltre un giorno lavorativo all'anno è a carico del Cliente alle tariffe indicate nell'Ordine o, in mancanza di tali tariffe, alle tariffe standard per servizi professionali in vigore. In via di eccezione, il Fornitore sostiene l'intero costo di un audit svolto a seguito di una violazione dei dati personali a esso imputabile o disposto da un'autorità di controllo competente, nonché di ogni audit aggiuntivo reso necessario da rilievi di non conformità a esso imputabili.

13.5 Limiti

L'audit non può estendersi ai dati, ai sistemi o alle informazioni di altri clienti del Fornitore, non può comprendere l'accesso non supervisionato ai sistemi di produzione, penetration test o scansioni di vulnerabilità senza previa autorizzazione scritta, e non può estendersi al codice sorgente, agli algoritmi o ai segreti industriali e commerciali del Fornitore, salvo nella misura strettamente necessaria a verificare una specifica misura di sicurezza e con modalità che ne preservino la riservatezza.

13.6 Rilievi

I rilievi dell'audit sono riservati e possono essere utilizzati soltanto per verificare la conformità al presente DPA. Il Fornitore presenta un piano di rimedio per ogni non conformità riscontrata entro trenta giorni dal ricevimento del rapporto e lo attua entro i tempi concordati.

Art. 14 — Restituzione e cancellazione dei Dati Personali del Cliente

14.1 Scelta del Cliente

Al termine della prestazione dei servizi relativi al trattamento, il Cliente sceglie se il Fornitore debba restituire i Dati Personali del Cliente o cancellarli. In mancanza di una scelta comunicata entro il periodo di recupero, il Fornitore procede alla cancellazione ai sensi dell'Articolo 14.3.

14.2 Periodo di recupero

Per trenta giorni dalla data di efficacia della risoluzione o della scadenza, il Cliente mantiene l'accesso alle funzioni di esportazione della Piattaforma per recuperare i Dati Personali del Cliente e gli altri Dati del Cliente in formati aperti strutturati, di uso comune e leggibili da dispositivo automatico. Non è applicato alcun onere di passaggio ad altro fornitore (switching) o di uscita, in conformità agli articoli 25 e 29 del regolamento (UE) 2023/2854 (Data Act). Ove il Cliente richieda la transizione assistita descritta nelle Master Terms, la transizione è completata entro trenta giorni dalla richiesta, con preavviso di avvio non superiore a due mesi.

14.3 Cancellazione

Il Fornitore cancella i Dati Personali del Cliente dagli ambienti di produzione entro trenta giorni dal termine del periodo di recupero, e dalle copie di backup al successivo ciclo di rotazione dei backup e comunque entro sessanta giorni dal termine del periodo di recupero. Fino al completamento della cancellazione, i dati restano protetti dalle misure dell'Allegato 2 e non sono accessibili per finalità diverse dal ripristino.

14.4 Certificato di cancellazione

Su richiesta scritta del Cliente formulata entro sei mesi dal termine del periodo di recupero, il Fornitore rilascia un certificato scritto di cancellazione entro quindici giorni dal completamento delle operazioni.

14.5 Conservazione richiesta dalla legge

Il Fornitore conserva, nella sua qualità di titolare ai sensi dell'Articolo 2.2, i dati richiesti da obblighi di legge, in particolare la documentazione contabile e fiscale e le evidenze di accettazione dei documenti contrattuali, per i periodi indicati nell'Informativa sulla Privacy. Tale conservazione non

costituisce trattamento per conto del Cliente ed è soggetta ad adeguate misure di sicurezza e alla limitazione di ogni ulteriore trattamento.

14.6 Risoluzione per mancato pagamento

La cancellazione prevista dal presente Articolo si applica anche quando il Contratto si risolve per mancato pagamento; il periodo di recupero è concesso per intero e non può essere subordinato al pagamento degli importi contestati, fermo restando il diritto del Fornitore di recuperarli con i mezzi previsti dalle Master Terms.

Art. 15 — Funzionalità di intelligenza artificiale, dati di addestramento e decisioni automatizzate

15.1 Esecuzione locale in via ordinaria

Le funzionalità di intelligenza artificiale della Piattaforma, comprese l'addestramento su documenti, l'assistente locale, il document store, la trascrizione vocale, il riconoscimento ottico dei caratteri e l'analisi delle immagini, sono eseguite in via ordinaria all'interno del tenant del Cliente o sull'infrastruttura gestita dal Fornitore all'interno del SEE, senza trasmissione di contenuti a fornitori terzi.

15.2 Nessun addestramento tra clienti

Il Fornitore non utilizza i Dati Personali del Cliente, né i contenuti caricati dal Cliente, per addestrare, mettere a punto, valutare o migliorare modelli, funzionalità o servizi messi a disposizione di altri clienti o utilizzati dal Fornitore per finalità proprie. Tale divieto può essere derogato soltanto sulla base di un documento di consenso separato, specifico e revocabile, sottoscritto dal Cliente a tale solo fine, che è l'unico veicolo di una simile autorizzazione: né l'accettazione del Contratto, né l'Ordine, né alcuna opzione all'interno della Piattaforma costituiscono tale consenso, e la sua revoca ha effetto per il futuro senza pregiudicare la liceità del trattamento già effettuato. I modelli addestrati sui contenuti del Cliente sono dedicati al tenant del Cliente e sono cancellati ai sensi dell'Articolo 14.

15.3 Inferenza remota

Ove una funzionalità richieda un modello che eccede la capacità dell'infrastruttura locale, l'inferenza remota è disattivata in via ordinaria e può essere abilitata soltanto su espressa istruzione scritta del Cliente. L'abilitazione è subordinata a: la previa indicazione del fornitore sulla Pagina dei Sub-responsabili con il termine di preavviso di cui all'Articolo 8.3; la sottoscrizione delle SCC nel modulo applicabile e il completamento di una TIA ove il fornitore sia stabilito al di fuori del SEE; l'impegno contrattuale del fornitore a non utilizzare i contenuti per finalità di addestramento proprie e a conservarli soltanto per il tempo strettamente necessario a produrre la risposta; e la minimizzazione dei contenuti trasmessi nel prompt.

15.4 Registrazioni vocali

Le registrazioni vocali trattate dalla funzionalità di trascrizione sono utilizzate esclusivamente per produrre il testo corrispondente e non sono utilizzate per identificare univocamente una persona fisica; esse non costituiscono pertanto dati biometrici ai sensi dell'articolo 4, punto 14), del GDPR. Le registrazioni sono cancellate una volta prodotta la trascrizione e comunque entro trenta giorni.

15.5 Ruoli ai sensi del regolamento sull'intelligenza artificiale

Ai fini del regolamento (UE) 2024/1689, il Fornitore è il fornitore delle funzionalità di intelligenza artificiale della Piattaforma ai sensi dell'articolo 3, punto 3), di tale regolamento e il Cliente è il deployer ai sensi dell'articolo 3, punto 4). Il Cliente è responsabile di informare le persone fisiche che interagiscono con l'assistente, e il Fornitore fornisce le corrispondenti informative di trasparenza a decorrere dalla data di applicazione dell'articolo 50 del regolamento (UE) 2024/1689. Le funzionalità di intelligenza artificiale non sono destinate a funzioni di sicurezza autonome e non sostituiscono i sistemi di sicurezza, di protezione e di emergenza dell'impianto.

15.6 Processo decisionale automatizzato

Il Fornitore non effettua, per conto del Cliente, processi decisionali automatizzati che producano effetti giuridici nei confronti degli interessati o che incidano su di essi in modo analogamente significativo. Ove il Cliente configuri la Piattaforma per supportare decisioni di tale natura, il Cliente è l'unico responsabile del rispetto dell'articolo 22 del GDPR, compresi l'intervento umano e le informazioni dovute agli interessati.

Art. 16 — Modelli di deployment On-Premise e VPS

16.1 Criterio di applicazione

Il presente DPA è concluso per ogni modello di deployment, compreso l'On-Premise, e il presente Articolo è l'unica fonte del suo ambito di applicazione ai modelli di deployment On-Premise e VPS: nessun altro documento del Contratto definisce tale ambito. L'applicazione del presente DPA ai modelli di deployment On-Premise e VPS dipende da un unico criterio: se il Fornitore abbia accesso effettivo ai Dati Personali del Cliente in forma intelligibile. La mera fornitura del software, il rilascio dei Grant di licenza (record di licenza firmato) e la verifica della loro validità non costituiscono, di per sé, trattamento di dati personali per conto del Cliente.

16.2 On-Premise senza accesso remoto

Ove la Piattaforma sia installata su sistemi del Cliente, o su un server fornito in comodato d'uso ubicato presso i locali del Cliente, e il Fornitore non abbia accesso remoto ai dati del Cliente e non svolga alcuna attività di supporto che comporti accesso a tali dati in forma intelligibile, il Fornitore non è né responsabile né titolare del trattamento dei dati trattati dal Cliente attraverso la Piattaforma e il presente DPA non si applica. In tale configurazione il Fornitore si impegna a che: il meccanismo di verifica della licenza trasmetta soltanto gli identificativi del Grant firmato, dell'installazione e del Bene Designato, e nessun dato di contenuto; si applichi un periodo di

tolleranza di trenta giorni ove la verifica non possa avere luogo; gli obblighi di riservatezza del Contratto e dell'accordo di non divulgazione restino pienamente applicabili. Il Cliente resta l'unico responsabile, in qualità di titolare del trattamento, dei dati trattati sui propri sistemi.

16.3 On-Premise con accesso di supporto remoto

Ove il Cliente richieda, autorizzi o abiliti attività di supporto, manutenzione, aggiornamento, diagnosi o correzione dei guasti, da remoto o in loco, che comportino accesso ai Dati Personali del Cliente in forma intelligibile, il Fornitore agisce come responsabile del trattamento e il presente DPA si applica a tali sole attività. In tal caso: ciascuna sessione è autorizzata preventivamente dal Cliente e registrata in un log di supporto che indica la data, l'operatore, la finalità e i sistemi a cui si è avuto accesso; il Fornitore accede soltanto ai dati strettamente necessari; sono preferite le sessioni remote supervisionate rispetto all'estrazione di copie; ogni copia acquisita a fini diagnostici è cancellata entro trenta giorni dalla chiusura dell'intervento e, su richiesta, viene rilasciato un certificato di cancellazione.

16.4 Cambiamento di configurazione

Se le circostanze di fatto mutano, e in particolare se l'accesso remoto ai dati in forma intelligibile viene abilitato dopo l'attivazione, l'Articolo 16.3 si applica automaticamente da tale data, senza ulteriori formalità, e le Parti registrano il cambiamento nel log di supporto. Nessuna Parte può invocare l'assenza di un accordo separato per escludere l'applicazione del presente DPA a trattamenti effettivamente avvenuti.

16.5 Modello di deployment VPS

Ove la Piattaforma sia fornita su un server privato virtuale gestito dal Fornitore, il Fornitore agisce come responsabile del trattamento e il presente DPA si applica integralmente. Il fornitore di tale infrastruttura è un Sub-responsabile, è identificato nell'Ordine prima dell'attivazione ed è indicato sulla Pagina dei Sub-responsabili ai sensi dell'Articolo 8.3; sono utilizzati soltanto fornitori con data centre situati all'interno del SEE.

16.6 Restituzione del server fornito in comodato

Alla restituzione di un server fornito in comodato d'uso, il Fornitore esegue una cancellazione sicura dei supporti di memorizzazione, secondo una procedura documentata, prima di ogni riutilizzo, e rilascia un verbale scritto della cancellazione. Prima del ritiro, al Cliente è data la possibilità di recuperare i propri dati ai sensi dell'Articolo 14.2.

Art. 17 — Responsabilità e manleve

17.1 Responsabilità verso gli interessati

L'articolo 82 del GDPR disciplina la responsabilità delle Parti verso gli interessati e non è modificato dal presente DPA. Nessuna disposizione del presente DPA o del Contratto limita i diritti degli interessati.

17.2 Responsabilità tra le Parti

Nei rapporti tra le Parti, la responsabilità derivante dal presente DPA è soggetta al limite complessivo di responsabilità stabilito nelle Master Terms, pari ai Corrispettivi pagati dal Cliente nei dodici mesi precedenti l'evento generatore della responsabilità. Tale limite non si applica, e non può essere invocato, nei casi di dolo o colpa grave, ai sensi dell'art. 1229 c.c., né con riferimento alla responsabilità di cui all'Articolo 17.1.

17.3 Regresso

Qualora una Parte abbia risarcito integralmente il danno subito da un interessato, essa ha diritto di richiedere all'altra Parte la parte del risarcimento corrispondente alla quota di responsabilità di quest'ultima, ai sensi dell'articolo 82, paragrafo 5, del GDPR.

17.4 Manleve

Il Cliente tiene indenne il Fornitore dalle conseguenze di istruzioni che violino la Normativa sulla Protezione dei Dati, dell'assenza di un'appropriata base giuridica, dell'omessa informativa dovuta agli interessati e del caricamento di contenuti in violazione dell'Articolo 5.6. Il Fornitore tiene indenne il Cliente dalle conseguenze dei trattamenti effettuati in violazione del presente DPA o in contrasto con le legittime istruzioni del Cliente.

17.5 Sanzioni amministrative

Ciascuna Parte sopporta le sanzioni amministrative a essa irrogate per violazioni imputabili alla propria condotta. Ove una sanzione sia irrogata per effetto di una condotta imputabile all'altra Parte, la Parte colpita può richiederne il rimborso nei limiti dell'Articolo 17.2.

Art. 18 — Durata, modifiche, ultrattività, legge applicabile e foro competente

18.1 Durata

Il presente DPA ha effetto dalla data di accettazione o di firma del Contratto e resta in vigore per tutto il tempo in cui il Fornitore tratta Dati Personali del Cliente, e in ogni caso fino al completamento delle operazioni di cancellazione di cui all'Articolo 14.

18.2 Modifiche

Le modifiche al presente DPA sono effettuate per iscritto. Il Fornitore può aggiornare unilateralmente gli Allegati 2 e 3, ai sensi degli Articoli 7.2 e 8.3, purché il livello di protezione non sia sostanzialmente ridotto; resta impregiudicato il diritto di opposizione del Cliente ai sensi dell'Articolo 8.4 per le modifiche all'Allegato 3.

18.3 Adeguamenti normativi

Se vengono adottate nuove clausole contrattuali tipo, nuove decisioni di esecuzione o nuovi provvedimenti vincolanti delle autorità di controllo, le Parti li adottano e adeguano gli Allegati entro i termini prescritti e, in assenza di un termine prescritto, entro novanta giorni. Ove uno strumento di trasferimento sia dichiarato invalido o sia ritirato, il Fornitore ne informa il Cliente senza ingiustificato ritardo, sospende ove necessario i trasferimenti interessati e propone uno strumento alternativo.

18.4 Ultrattività

Gli Articoli 6, 12, 14 e 17 sopravvivono alla cessazione del presente DPA, insieme a ogni disposizione che per sua natura sia destinata a sopravvivere.

18.5 Legge applicabile e foro competente

Il presente DPA è regolato dalla legge italiana. Per i clienti professionali, in ogni paese, il Tribunale di Bergamo ha giurisdizione esclusiva su ogni controversia derivante dal presente DPA o a esso connessa, ai sensi dell'articolo 25 del regolamento (UE) 1215/2012, fermo restando il diritto del Fornitore di richiedere misure cautelari e provvedimenti inibitori dinanzi a qualsiasi giudice competente e ferma restando la facoltà di arbitrato prevista dalle Master Terms. Restano impregiudicate le tutele imperative dei consumatori, compresa la competenza del giudice del luogo di residenza del consumatore. Ove le SCC si applichino, la legge da esse indicata e la loro elezione di foro prevalgono per le materie che esse disciplinano, e resta impregiudicato il diritto degli interessati di agire in giudizio ai sensi delle SCC.

18.6 Clausola di salvaguardia

Se una disposizione del presente DPA è dichiarata invalida o inefficace, le restanti disposizioni restano in vigore e le Parti sostituiscono la disposizione invalida con una disposizione valida che realizzi nel modo più prossimo possibile il medesimo effetto economico e giuridico.

Art. 19 — Punti di contatto, comunicazioni e registri

19.1 Punto di contatto del Fornitore

Le comunicazioni in materia di protezione dei dati indirizzate al Fornitore sono inviate a support@devibrain.com con il riferimento "GDPR" nell'oggetto, oppure tramite posta elettronica certificata a devibrain@pec.it, oppure con lettera raccomandata a DEVIBRAIN S.R.L., Via Coghetti 6, 24128 Bergamo (BG), Italia. Anche le notifiche di violazioni dei dati personali e le richieste delle autorità pubbliche sono inviate a tale indirizzo e sono trattate in via prioritaria.

19.2 Responsabile della protezione dei dati

Alla data della versione il Fornitore non ha nominato un responsabile della protezione dei dati, non ricorrendo le condizioni dell'articolo 37, paragrafo 1, del GDPR, e designa il punto di contatto di cui all'Articolo 19.1 quale riferimento per le questioni di protezione dei dati. Ove tali condizioni

ricorrano, il Fornitore nomina un responsabile della protezione dei dati, ne pubblica i dati di contatto sulla Pagina dei Sub-responsabili e li comunica al Cliente.

19.3 Punto di contatto del Cliente

Il punto di contatto del Cliente è quello indicato nell'Ordine o, in mancanza di tale indicazione, l'amministratore dell'account del Cliente sulla Piattaforma. Il Cliente mantiene aggiornato tale punto di contatto ed è responsabile delle conseguenze di un indirizzo non valido o non presidiato, anche in relazione alle comunicazioni di cui agli Articoli 8.3 e 10.1.

19.4 Forma delle comunicazioni

Le comunicazioni previste dal presente DPA sono valide se inviate per posta elettronica ai punti di contatto, con copia nell'area notifiche della Piattaforma. Esse hanno effetto al ricevimento o, se successiva, alla data in esse indicata.

19.5 Registri dei trattamenti

Ciascuna Parte tiene il registro delle attività di trattamento richiesto dall'articolo 30 del GDPR. Il Fornitore mette a disposizione del Cliente, su richiesta e una volta all'anno, la parte del proprio registro di cui all'articolo 30, paragrafo 2, del GDPR che riguarda il Cliente.

Art. 20 — Approvazione specifica delle clausole

20.1 Clausole soggette ad approvazione specifica

Ai sensi degli artt. 1341 e 1342 c.c., il Cliente dichiara di aver letto e approva specificamente le seguenti disposizioni del presente DPA: Articolo 5.2 (corrispettivi per ulteriori istruzioni), Articolo 5.3 (sospensione delle istruzioni ritenute illegittime), Articolo 7.2 (aggiornamento unilaterale delle misure di sicurezza), Articolo 7.3 (responsabilità del Cliente), Articoli 8.1, 8.3, 8.4 e 8.6 (autorizzazione generale, modifica unilaterale e sostituzione urgente dei Sub-responsabili), Articolo 9.3 (corrispettivi per l'assistenza aggiuntiva), Articoli 13.2, 13.4 e 13.5 (procedura, costi e limiti dell'audit), Articolo 14.3 (termini di cancellazione), Articolo 17.2 (limitazione di responsabilità tra le Parti), Articolo 17.4 (manleve), Articolo 18.2 (modifica unilaterale degli Allegati) e Articolo 18.5 (legge applicabile, foro esclusivo e riserva di arbitrato).

20.2 Accettazione digitale

Ove il presente DPA sia accettato attraverso il flusso self-service, l'approvazione specifica di cui all'Articolo 20.1 è prestata in un passaggio separato, distinto dall'accettazione del documento nel suo complesso, confermata da un codice monouso inviato all'indirizzo di posta elettronica della persona che accetta e registrata nell'evidenza di accettazione unitamente alla marca temporale, all'indirizzo del protocollo internet, allo user agent, all'account e all'hash e alla versione del documento.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

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
_____	_____

Allegato 1 — Descrizione del trattamento

Il presente Allegato soddisfa l'articolo 28, paragrafo 3, del GDPR e costituisce l'Allegato I.B delle SCC ove le SCC si applichino.

A1.1 Oggetto, natura e finalità

L'oggetto del trattamento sono i dati personali contenuti nei contenuti che il Cliente e i suoi Utenti Autorizzati inseriscono, caricano o generano attraverso la Piattaforma. La natura del trattamento consiste in raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, estrazione, consultazione, uso, trasmissione, limitazione e cancellazione, effettuate con mezzi automatizzati, unitamente a hosting, backup, monitoraggio della sicurezza, supporto tecnico e, ove attivate, inferenza locale di intelligenza artificiale e addestramento per singolo tenant. La finalità del trattamento è la fornitura, il funzionamento, la manutenzione, la sicurezza e il supporto della Piattaforma per conto del Cliente, in conformità al Contratto e alle istruzioni documentate del Cliente, e per nessun'altra finalità.

A1.2 Categorie di interessati

• Utenti Autorizzati del Cliente, compresi ingegneri, operatori di impianto, tecnici di manutenzione, personale della qualità e amministratori di sistema.

• Dipendenti, collaboratori, lavoratori somministrati e appaltatori del Cliente i cui dati compaiono in dashboard, allarmi, ricette, istruzioni di lavoro, assegnazioni di turno, audit trail o contenuti multimediali gestiti attraverso la Piattaforma.

• Dipendenti e rappresentanti dei fornitori, dei system integrator e dei clienti del Cliente, ove i loro dati compaiano nei contenuti caricati dal Cliente.

• Ogni altra persona fisica i cui dati il Cliente decida di includere nei contenuti che carica, compresi i dati che compaiono nei documenti trattati dalle funzionalità di addestramento su documenti e di document store.

A1.3 Categorie di dati personali

Categoria	Esempi di dati	Fonte
Dati identificativi	nome, cognome, numero di matricola o di badge, codice personale	creazione dell'account e contenuti caricati dal Cliente
Dati di contatto	indirizzo di posta elettronica aziendale, numero di telefono, reparto, sito	creazione dell'account e contenuti caricati dal Cliente
Dati di account e di autenticazione	nome utente, hash con sale della password, ruolo e permessi, fattori di autenticazione a più fattori, identificativi di sessione	utilizzo della Piattaforma
Dati professionali	mansione, qualifica, turno, impianto, linea, competenza per una data operazione	contenuti caricati dal Cliente
Dati di attività all'interno del tenant	registrazioni di accesso e disconnessione, azioni compiute, marche temporali, indirizzo del protocollo internet, dispositivo e browser utilizzati, audit trail delle modifiche	utilizzo della Piattaforma
Dati di contenuto	documenti, disegni, immagini, video, registrazioni audio, ricette, testi degli allarmi, annotazioni e campi di testo libero caricati o generati dal Cliente	contenuti caricati dal Cliente
Dati tecnici e diagnostici riferibili a una persona	log applicativi, segnalazioni di errore e ticket di supporto ove contengano dati di una persona identificata o identificabile	utilizzo della Piattaforma e supporto

A1.4 Categorie particolari di dati personali

Nessuna. Il Cliente è istruito ai sensi dell'Articolo 5.6 a non caricare categorie particolari di dati personali né dati relativi a condanne penali e reati, salvo quanto espressamente concordato per iscritto nell'Ordine unitamente alle misure supplementari richieste dal rischio. Le registrazioni vocali trattate dalla funzionalità di trascrizione non sono utilizzate per l'identificazione univoca di una persona fisica e pertanto non costituiscono dati biometrici.

A1.5 Operazioni di trattamento per modulo

Modulo	Operazioni di trattamento	Dati personali tipicamente coinvolti
3D Builder	creazione, conservazione ed esportazione di modelli tridimensionali, proprietà, diagnostiche e viewpoint vincolati a un Bene Designato	dati identificativi e professionali degli operatori mostrati nelle diagnostiche e negli audit trail
Chart Builder	creazione, conservazione ed esportazione di grafici e tracce	dati degli operatori associati agli eventi registrati
Tool Builder	gestione di documenti, contenuti multimediali, ricette e allarmi	dati identificativi e di contatto presenti nei documenti, nei contenuti multimediali e nei testi degli allarmi
Smart Process	conversione e analisi di schemi e disegni di impianto	dati delle persone nominate nei disegni e nella documentazione di accompagnamento
UI Designer	progettazione e conservazione di dashboard e interfacce	dati degli operatori mostrati nelle interfacce
Assistente di intelligenza artificiale, document store, trascrizione e riconoscimento ottico dei caratteri	indicizzazione, trascrizione, estrazione e addestramento per singolo tenant sui contenuti caricati dal Cliente	qualsiasi dato personale contenuto nei contenuti caricati dal Cliente

Modulo	Operazioni di trattamento	Dati personali tipicamente coinvolti
Console e license manager	gestione degli Utenti Autorizzati, dei ruoli, dei Grant di licenza firmati e del provisioning del tenant	dati identificativi, di contatto e di account degli Utenti Autorizzati
Supporto tecnico	gestione dei ticket, diagnostiche e sessioni remote supervisionate	dati presenti nei sistemi ai quali si è avuto accesso durante l'intervento

A1.6 Frequenza e durata

Il trattamento è continuativo per i modelli di deployment ospitati e occasionale per gli interventi di supporto nel modello di deployment On-Premise. La durata è quella del Contratto, più un periodo di recupero di trenta giorni, la cancellazione dagli ambienti di produzione entro ulteriori trenta giorni e la purga delle copie di backup al successivo ciclo di rotazione e comunque entro sessanta giorni dal termine del periodo di recupero.

A1.7 Conservazione all'interno della Piattaforma

I dati di contenuto sono conservati per tutto il tempo in cui il Cliente li mantiene nel proprio tenant e sono cancellati quando il Cliente li cancella o quando scadono i termini di cui all'Articolo 14. I log applicativi e di accesso sono conservati per dodici mesi e successivamente cancellati o aggregati in una forma che non consente l'identificazione. Le copie di backup sono conservate per trenta giorni con rotazione continua. Le registrazioni vocali sono cancellate una volta prodotta la trascrizione e comunque entro trenta giorni.

A1.8 Trasferimenti ai Sub-responsabili

L'oggetto, la natura e la durata dei trattamenti effettuati dai Sub-responsabili sono quelli indicati nell'Allegato 3 per ciascuno di essi e sono limitati a quanto necessario per il servizio a essi affidato.

Allegato 2 — Misure tecniche e organizzative di sicurezza

Il presente Allegato descrive le misure attuate ai sensi dell'articolo 32 del GDPR e costituisce l'Allegato II delle SCC ove le SCC si applichino. Le misure sono vincolanti per il Fornitore e possono essere aggiornate soltanto ai sensi dell'Articolo 7.2.

A2.1 Pseudonimizzazione e cifratura

I dati in transito sono protetti da transport layer security versione 1.2 o superiore, con certificati gestiti automaticamente e rinnovati prima della scadenza, su ogni interfaccia pubblica e tra i componenti esposti all'esterno dell'host. Gli host di produzione utilizzano la cifratura integrale dei volumi contenenti i dati. Le copie di backup sono cifrate con l'advanced encryption standard con chiave di lunghezza 256 bit, e le chiavi sono custodite separatamente dai backup. Le password sono conservate soltanto come hash unidirezionali con sale. I Grant di licenza sono firmati con crittografia a curva ellittica sulla curva P-256; la chiave privata di firma è custodita esclusivamente nella console di gestione, mai negli ambienti tenant, e non è mai inclusa nelle immagini distribuite ai clienti. I Dati di Utilizzo e la telemetria sono pseudonimizzati ove tecnicamente possibile.

A2.2 Riservatezza e controllo degli accessi

L'accesso avviene con credenziali individuali e nominative, con permessi basati sui ruoli e secondo il principio del privilegio minimo. L'autenticazione a più fattori è richiesta per l'accesso amministrativo alla console e all'infrastruttura. Le sessioni scadono dopo un periodo di inattività. I permessi amministrativi sono riesaminati almeno ogni sei mesi e revocati il giorno stesso in cui cessa il rapporto. L'accesso alla produzione è concesso soltanto per il tempo necessario a gestire una richiesta ed è registrato. I segreti e le credenziali non sono conservati nei repository del codice sorgente.

A2.3 Integrità e separazione dei trattamenti

Ciascun tenant viene eseguito in un gruppo di container dedicato, con database proprio e rete propria, senza stato applicativo condiviso tra tenant. È imposta la segregazione tra ambienti di sviluppo, test e produzione; i dati di produzione non sono utilizzati per lo sviluppo o per i test e, ove una copia sia strettamente necessaria, essa è previamente anonimizzata. Le modifiche al software seguono un processo documentato con controllo di versione, revisione tra pari e test end-to-end prima del rilascio. Le azioni amministrative sono registrate in un audit trail a prova di manomissione. Le evidenze di accettazione dei documenti contrattuali sono conservate in forma a prova di manomissione e mantenute per dieci anni.

A2.4 Sicurezza di rete e delle applicazioni

L'infrastruttura è esposta attraverso un unico componente di frontiera irrobustito; le porte applicative non sono pubblicate direttamente. Le reti interne sono segmentate per funzione e per tenant. I front end applicativi non caricano font, script, fogli di stile o altre risorse da content delivery network esterne in fase di esecuzione, essendo tutte le risorse statiche ospitate localmente; tale vincolo, adottato per gli ambienti industriali air-gapped, previene anche trasferimenti non voluti di identificativi di rete a terzi. Le content security policy limitano le origini consentite al browser. Le dipendenze sono monitorate e aggiornate; le correzioni di sicurezza sono applicate entro i termini graduati per gravità secondo il common vulnerability scoring system stabiliti all'Articolo 7.3 del Service Level Agreement (IUX-IT-30), che è l'unica fonte di tali termini e che il presente Allegato non riduce.

A2.5 Disponibilità, backup e continuità

I backup sono eseguiti quotidianamente, conservati per trenta giorni con rotazione continua e archiviati separatamente dai sistemi di produzione all'interno del SEE. I test di ripristino sono svolti almeno due volte l'anno e i risultati sono documentati. Gli obiettivi di ripristino e i livelli di disponibilità sono quelli indicati nel Service Level Agreement (IUX-IT-30). L'infrastruttura è protetta contro le interruzioni di alimentazione e monitorata per la saturazione delle risorse di memorizzazione e di calcolo.

A2.6 Gestione degli incidenti

È in essere una procedura documentata di gestione degli incidenti che definisce classificazione, escalation, contenimento, eradicazione, ripristino e revisione post-incidente, unitamente alla notifica al Cliente entro quarantotto ore prevista dall'Articolo 10.1. È designato un punto di contatto unico per gli incidenti di sicurezza. I log e le evidenze rilevanti per un incidente sono conservati per il tempo necessario all'indagine e all'esercizio dei diritti.

A2.7 Misure sul personale

Il personale è vincolato da impegni scritti di riservatezza, riceve formazione in materia di protezione dei dati e di sicurezza delle informazioni al momento dell'assunzione e periodicamente in seguito, ed è soggetto a una procedura documentata di offboarding che prevede la revoca immediata degli accessi e la restituzione delle apparecchiature. L'accesso ai Dati Personali del Cliente è concesso soltanto in base al principio della necessità di conoscere.

A2.8 Gestione dei fornitori

I Sub-responsabili sono selezionati sulla base di una due diligence documentata che copre la sicurezza, il luogo del trattamento e le garanzie per i trasferimenti, sono vincolati da contratti scritti ai sensi dell'articolo 28, paragrafo 4, del GDPR e sono rivalutati almeno una volta l'anno. Sono preferiti i fornitori con trattamento localizzato all'interno del SEE, e un fornitore stabilito al di fuori del SEE è incaricato soltanto previa sottoscrizione delle SCC e previa TIA con esito positivo.

A2.9 Sicurezza fisica

I sistemi sono ospitati in locali ad accesso controllato, in sale riservate alle apparecchiature informatiche, con accesso limitato al personale autorizzato e registrato. I supporti di memorizzazione giunti a fine vita sono cancellati secondo una procedura documentata o distrutti fisicamente, con verbale scritto.

A2.10 Minimizzazione, qualità e portabilità dei dati

La Piattaforma consente al Cliente di configurare i campi raccolti, di correggere e cancellare i dati e di esportarli in formati aperti strutturati, di uso comune e leggibili da dispositivo automatico, compresi i formati utilizzati per modelli, grafici, documenti e immagini gestiti dalle applicazioni. Le funzioni di cancellazione operano immediatamente sull'ambiente di produzione e sulle copie di backup attraverso la rotazione descritta all'Articolo 14.3.

A2.11 Governance e accountability

Il Fornitore mantiene il registro delle attività di trattamento richiesto dall'articolo 30, paragrafo 2, del GDPR, un registro degli incidenti di sicurezza, un registro dei rapporti di sub-responsabilità e la documentazione della TIA descritta nell'Allegato 5. Le misure del presente Allegato sono riesaminate almeno una volta l'anno e a seguito di ogni incidente significativo o di ogni modifica sostanziale dell'architettura.

Allegato 3 — Sub-responsabili

A3.1 Elenco pubblicato

L'elenco dei Sub-responsabili in essere è pubblicato sulla Pagina dei Sub-responsabili all'indirizzo https://www.industryux.com/legal/sub-processors, che indica per ciascuno di essi l'identità, la sede legale, il servizio affidato, il luogo del trattamento, le categorie di dati interessate e lo strumento di trasferimento ove applicabile, unitamente alla data dell'ultimo aggiornamento. La pagina consente l'iscrizione alle notifiche di modifica via posta elettronica. Le modifiche sono disciplinate dall'Articolo 8.

A3.2 Sub-responsabili autorizzati alla data della versione

Alla data del presente Allegato non è attivo alcun sub-responsabile esterno. I Dati Personali del Cliente sono trattati esclusivamente dalla funzione operativa interna del Fornitore, descritta nella tabella che segue. L'incarico di qualsiasi Sub-responsabile esterno è soggetto al preavviso di trenta giorni di cui all'Articolo 8.3 e al diritto di opposizione del Cliente di cui all'Articolo 8.4, e il Sub-responsabile è nominato — con la sua identità, sede legale, servizio affidato, luogo del trattamento, categorie di dati interessate e strumento di trasferimento — in tale comunicazione e sulla Pagina dei Sub-responsabili prima che inizi a trattare Dati Personali del Cliente.

Sub-responsabile	Servizio affidato	Luogo del trattamento	Categorie di dati	Strumento di trasferimento
DEVIBRAIN S.R.L. — funzione operativa interna	hosting, backup, monitoraggio, supporto di secondo livello degli ambienti Enterprise Online su infrastruttura gestita direttamente dal Fornitore	Bergamo, Italia (SEE)	tutti i dati descritti nell'Allegato 1	non applicabile, nessun trasferimento

A3.3 Dichiarazioni

Alla data della versione nessun terzo ha accesso ai Dati Personali del Cliente. L'inferenza remota è disattivata in via ordinaria e nessun Dato Personale del Cliente è trasmesso a un fornitore al di fuori del SEE in assenza dell'espressa istruzione e delle garanzie previste all'Articolo 15.3; un fornitore di inferenza remota diventa Sub-responsabile soltanto una volta nominato ai sensi dell'Articolo A3.2. Ove sia attivato il modello di deployment VPS, il fornitore dell'infrastruttura è incaricato come Sub-responsabile ai sensi degli Articoli 8.3 e 16.5. Nel modello di deployment On-Premise non è incaricato alcun Sub-responsabile, restando i dati sui sistemi del Cliente.

A3.4 Fornitori del Fornitore in qualità di titolare

I fornitori che seguono non sono Sub-responsabili ai sensi del presente DPA, poiché trattano dati rispetto ai quali il Fornitore agisce come titolare ai sensi dell'Articolo 2.2. Essi sono elencati in questa sede a fini di trasparenza e sono descritti nell'Informativa sulla Privacy.

Fornitore	Servizio	Luogo del trattamento	Ruolo
Nexi Payments S.p.A.	accettazione e gestione dei pagamenti con carta per gli abbonamenti self-service	Italia (SEE)	titolare autonomo per l'operazione di pagamento, responsabile del trattamento per i dati trasmessi dal Fornitore

Allegato 4 — Clausole contrattuali tipo 2021/914

Nota sulla versione ufficiale italiana. La decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021, esiste in versione italiana ufficiale pubblicata nella Gazzetta ufficiale dell'Unione europea: è quella versione, e non la presente traduzione, che si intende incorporata per rinvio ai sensi dell'Articolo A4.1 e che fa fede tra le Parti. La traduzione italiana delle SCC eventualmente riportata o richiamata nel presente Allegato ha valore di cortesia.

A4.1 Incorporazione

Ove abbia luogo un trasferimento di Dati Personali del Cliente verso un paese terzo non coperto da una decisione di adeguatezza, le Parti sottoscrivono le SCC, che sono incorporate nel presente DPA per rinvio e completate secondo quanto stabilito nel presente Allegato. Le Parti si considerano aver firmato le SCC alla data di accettazione o di firma del Contratto, per i moduli applicabili al loro rapporto. In caso di conflitto, le SCC prevalgono sul presente DPA.

A4.2 Moduli applicabili

Modulo	Configurazione	Applicazione al rapporto IndustryUX
Modulo 1 — da titolare a titolare	esportatore titolare, importatore titolare	residuale; si applica soltanto agli scambi di dati di contatto aziendali con partner stabiliti al di fuori del SEE che agiscono come titolari autonomi
Modulo 2 — da titolare a responsabile	esportatore titolare, importatore responsabile	si applica ove il Fornitore agisca come titolare ai sensi dell'Articolo 2.2 e affidi un'operazione di trattamento a un fornitore stabilito al di fuori del SEE
Modulo 3 — da responsabile a responsabile	esportatore responsabile, importatore sub-responsabile	si applica ove il Fornitore, in qualità di responsabile per il Cliente, incarichi un Sub-responsabile stabilito al di fuori del SEE, in particolare un fornitore di inferenza di intelligenza artificiale o di capacità cloud; alla data della versione non è incaricato alcun Sub-responsabile di tale tipo
Modulo 4 — da responsabile a titolare	esportatore responsabile stabilito nel SEE, importatore titolare stabilito al di fuori del SEE	si applica ove il Cliente sia un titolare stabilito al di fuori del SEE e il Fornitore, stabilito in Italia, gli renda disponibili o gli restituisca Dati Personali del Cliente

A4.3 Opzioni selezionate

Clausola	Opzione selezionata
Clausola 7 — clausola di adesione	inclusa; ulteriori parti possono aderire con l'accordo delle parti esistenti
Clausola 9 — ricorso a sub-responsabili, Moduli 2 e 3	Opzione 2, autorizzazione scritta generale, con termine di preavviso di trenta giorni come previsto all'Articolo 8.3
Clausola 11 — mezzi di ricorso	il paragrafo facoltativo relativo all'organismo indipendente di risoluzione delle controversie non è selezionato

Clausola	Opzione selezionata
Clausola 13 — controllo	l'autorità di controllo competente è il Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Roma, Italia, essendo l'esportatore stabilito in Italia; ove l'esportatore sia il Cliente stabilito in un altro Stato membro, è competente l'autorità di controllo di tale Stato membro
Clausola 17 — legge applicabile	Opzione 1, legge italiana
Clausola 18 — foro competente e giurisdizione	i giudici italiani, fermo restando il diritto degli interessati di agire dinanzi ai giudici del loro luogo di residenza abituale

A4.4 Corrispondenza degli allegati

Allegato delle SCC	Contenuto	Fonte
Allegato I.A — elenco delle parti	identità, indirizzo, punto di contatto, attività e ruolo delle parti	i dati identificativi contenuti nel preambolo del presente DPA e nell'Ordine per il Cliente; per l'importatore, i dati pubblicati sulla Pagina dei Sub-responsabili e indicati nella comunicazione di cui all'Articolo 8.3
Allegato I.B — descrizione del trasferimento	categorie di interessati e di dati, frequenza, natura, finalità, conservazione, sub-responsabilità	Allegato 1 del presente DPA
Allegato I.C — autorità di controllo competente	individuazione dell'autorità	clausola 13 come completata all'Articolo A4.3

Allegato delle SCC	Contenuto	Fonte
Allegato II — misure tecniche e organizzative	misure di sicurezza dell'importatore	Allegato 2 del presente DPA e le misure dell'importatore indicate nella comunicazione di cui all'Articolo 8.3
Allegato III — elenco dei sub-responsabili, Modulo 3	identità e descrizione del trattamento	Allegato 3 del presente DPA e Pagina dei Sub-responsabili

A4.5 EU-US Data Privacy Framework

La decisione di adeguatezza del 10 luglio 2023 relativa all'EU-US Data Privacy Framework è in vigore ma non è adottata come base primaria di trasferimento per il rapporto disciplinato dal presente DPA. Le ragioni sono le seguenti, valutate alla data della versione: la sentenza della Corte Suprema degli Stati Uniti del 29 giugno 2026 nel caso Trump v. Slaughter, che ha rimosso la protezione contro la rimozione senza giusta causa dei membri della Federal Trade Commission, l'autorità sulla quale poggiano i meccanismi di applicazione e di ricorso di tale framework; la perdita del quorum del Privacy and Civil Liberties Oversight Board dal gennaio 2025, che impedisce le revisioni annuali del meccanismo di ricorso; e l'impugnazione proposta il 31 ottobre 2025 dinanzi alla Corte di giustizia dell'Unione europea avverso la sentenza del Tribunale dell'Unione europea del 3 settembre 2025 nel caso Latombe, tuttora pendente, che rende realistica la prospettiva di un ulteriore annullamento della decisione di adeguatezza. Di conseguenza il Fornitore adotta le SCC combinate con la TIA di cui all'Allegato 5 quale base primaria per i trasferimenti verso gli Stati Uniti, e tratta la certificazione nell'ambito di tale framework come elemento aggiuntivo di valutazione. Qualora la decisione di adeguatezza sia annullata o ritirata, i trasferimenti già coperti dalle SCC e dalla TIA proseguono senza interruzione.

A4.6 Misure supplementari

Le misure supplementari adottate per i trasferimenti basati sulle SCC sono, come minimo: la cifratura in transito e a riposo con chiavi custodite all'interno del SEE e inaccessibili all'importatore; la minimizzazione dei dati trasmessi, in particolare nei prompt inviati ai fornitori di inferenza remota; il divieto contrattuale per l'importatore di utilizzare i dati per finalità proprie o di conservarli oltre il tempo necessario; gli obblighi di trasparenza e di contestazione stabiliti all'Articolo 12; e il riesame periodico della TIA ai sensi dell'Allegato 5.

Allegato 5 — Valutazione d'impatto sul trasferimento

A5.1 Finalità e metodo

Prima di ogni trasferimento basato sulle SCC, e periodicamente in seguito, il Fornitore effettua e documenta una valutazione d'impatto sul trasferimento seguendo il metodo in sei fasi delle Raccomandazioni 01/2020 del Comitato europeo per la protezione dei dati sulle misure che integrano gli strumenti di trasferimento. La TIA è un documento di accountability interna ai sensi degli articoli 5, paragrafo 2, e 24 del GDPR; non è pubblicata, ma è messa a disposizione del Cliente su richiesta ai sensi dell'Articolo 13.1 e dell'autorità di controllo competente su richiesta.

A5.2 Le sei fasi e il contenuto del registro

Fase	Domanda cui rispondere	Contenuto che il registro deve indicare
1. Mappare il trasferimento	quali dati vanno dove, a chi e per quale finalità	identificazione dell'esportatore e dell'importatore, il modulo delle SCC utilizzato, le categorie di dati e di interessati, i volumi, la frequenza, il percorso tecnico dei dati, i trasferimenti successivi ed eventuali accessi da remoto da un paese terzo
2. Individuare lo strumento di trasferimento	su quale strumento del Capo V del GDPR ci si basa	il modulo delle SCC sottoscritto, la data di sottoscrizione, l'eventuale decisione di adeguatezza invocata come elemento aggiuntivo e le ragioni per cui non è adottata come base primaria
3. Valutare la legge e la prassi del paese terzo	se il diritto del paese di destinazione comprometta l'efficacia dello strumento	analisi della legislazione sulla sorveglianza applicabile all'importatore, in particolare delle disposizioni sull'accesso delle autorità pubbliche per finalità di sicurezza nazionale e sugli ordini di produzione extraterritoriali, dei rimedi disponibili per i non cittadini, della prassi effettiva documentata da fonti pubbliche e delle dichiarazioni ottenute dall'importatore, unitamente a una conclusione motivata sul livello di rischio
4. Individuare le misure supplementari	quali misure tecniche, contrattuali e organizzative riducono il rischio residuo	le misure tecniche quali cifratura forte con chiavi custodite nel SEE, pseudonimizzazione e minimizzazione dei contenuti trasmessi; le misure contrattuali quali obblighi di trasparenza, contestazione, notifica e audit; le misure organizzative quali policy interne, formazione e riesame periodico; e la valutazione della loro sufficienza

Fase	Domanda cui rispondere	Contenuto che il registro deve indicare
5. Adottare le misure e formalizzarle	quali passaggi procedurali sono stati completati	le modifiche apportate al contratto con l'importatore, le configurazioni tecniche attivate, la data di adozione, il titolare interno della misura e le evidenze di attuazione
6. Rivalutare a intervalli appropriati	quando la valutazione deve essere riesaminata	la data di riesame, almeno annuale, e i fattori che impongono un riesame immediato, vale a dire una modifica legislativa nel paese terzo, un incidente, una richiesta di un'autorità pubblica, un cambio di importatore o una decisione di un giudice o di un'autorità di controllo che incida sullo strumento di trasferimento

A5.3 Esito e conseguenze

Il registro si conclude con uno di tre esiti: trasferimento consentito con le misure ordinarie; trasferimento consentito subordinatamente alle misure aggiuntive individuate, da attuare prima dell'inizio del trasferimento; trasferimento non consentito, nel qual caso il trasferimento non è avviato o, se già iniziato, è sospeso e il Cliente è informato senza ingiustificato ritardo ai sensi dell'Articolo 18.3. La conclusione è datata, attribuita a una persona responsabile nominativamente individuata e approvata dal legale rappresentante del Fornitore.

A5.4 Conservazione e aggiornamento

I registri della TIA, e le loro versioni successive, sono conservati per l'intera durata del trasferimento e per cinque anni dopo la sua cessazione. Il registro delle TIA in essere, che indica per ciascuna di esse l'importatore, il paese, la data dell'ultimo riesame e l'esito, fa parte della documentazione di accountability di cui all'Articolo A2.11.

Nota di validazione

Il presente documento è una versione release candidate 1.2 del corpus contrattuale IndustryUX, predisposta sulla base della normativa, della giurisprudenza e dei provvedimenti delle autorità di controllo in vigore al 10 agosto 2026. Non costituisce un parere legale. Prima di essere utilizzato con clienti reali deve essere validato da un avvocato qualificato e, per le parti relative alla protezione dei dati personali, da un professionista qualificato in materia di protezione dei dati, il quale deve verificare in particolare la corrispondenza tra le misure descritte nell'Allegato 2 e quelle effettivamente attuate, la completezza dell'elenco dell'Allegato 3 con riferimento all'infrastruttura in produzione e l'attualità della valutazione di cui all'Articolo A4.5 relativa ai trasferimenti verso gli Stati Uniti, che dipende da sviluppi ancora in corso.

Changelog

Versione	Data	Modifiche
1.0	2026-08-10	Prima versione release candidate
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; riferimenti di canale aggiornati di conseguenza
1.2	2026-08-11	Traduzione italiana di cortesia della versione inglese 1.2

IUX-IT-31 · v1.2 · 2026-08-11 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.