JURA Club — Fascicolo legale

Titoli Digitali Certificati — istruttoria tecnica e quesiti per il legale incaricato

Predisposto per: **JURA Club** (società titolare: [CLIENTE — da compilare])

Data di emissione: 30/07/2026

> **BOZZA — documenti tecnico-preparatori, NON pareri legali.** Nessun documento contenuto in questo fascicolo costituisce parere legale vincolante o consulenza in materia di servizi finanziari, antiriciclaggio o protezione dei dati. Tutti i documenti sono da validare con legale abilitato prima di qualsiasi uso e da emettere a nome del Cliente.

Indice del fascicolo

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, committente e titolare della piattaforma JURA Club), quale istruttoria tecnica a supporto dell’incarico legale; da validare con legale abilitato prima di qualsiasi uso. Non costituisce parere legale né consulenza in materia di servizi di investimento, antiriciclaggio o protezione dei dati. Le qualificazioni giuridiche sono riservate al legale incaricato dal Cliente. Versione: v0.4 · Data: 2026-07-30 · Stato: DRAFT interno · Riservato Novità v0.4: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del

> placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.3: aggiunti i quesiti Q30 (Decreto Fintech / registri per la circolazione digitale) e Q31 (Linee guida EDPB 02/2025); corretta la dicitura sul permissioning.

09 · Pacchetto di consegna per il legale — Istruttoria e quesiti (T-002 / T-060)

0. Modello dei ruoli — chi è il soggetto obbligato

> **Premessa fondamentale.** Gli obblighi regolamentari (qualificazione degli strumenti, offerta al pubblico, AML, GDPR, fiscalità, tutela del consumatore) ricadono sul **Cliente**, in quanto **titolare e operatore** della piattaforma. A **controllare ed emettere** i Titoli Digitali Certificati è la piattaforma **JURA Club** (operata dal Cliente), tramite un'infrastruttura **DLT propria oppure noleggiata da terze parti** (es. una rete pubblica EVM come Polygon); **il fornitore tecnico esterno non controlla i Titoli né la DLT; il controllo è di JURA Club o del provider DLT terzo**. Il **fornitore tecnico esterno** è unicamente il fornitore tecnologico che sviluppa il software della piattaforma per conto del Cliente. La corretta individuazione dei ruoli è essenziale per indirizzare correttamente il parere.

Soggetto	Ruolo	Posizione giuridica
Cliente / Committente *(dati in §0.1)*	**Titolare e operatore** della piattaforma JURA Club; **soggetto emittente/promotore** dei Titoli Digitali; **parte** dei contratti con utenti, creator e acquirenti	**Titolare del trattamento** dei dati personali (data controller); soggetto cui si riferiscono l'eventuale qualifica **CASP/VASP** e gli **obblighi AML**; soggetto di riferimento per **MiCAR/TUF**. Sede in **Italia** → disciplina **italiana e UE** in via diretta
Fornitore tecnico esterno	**Fornitore tecnologico / sviluppatore** della piattaforma per conto del Cliente (contratto di	Potenziale **responsabile del trattamento (art. 28 GDPR)** per i soli trattamenti svolti per

	sviluppo software); titolare del software di base, con licenza d'uso a JURA Club	conto del Cliente (es. sviluppo, hosting, manutenzione), da regolare con **DPA**. **Non** è titolare del prodotto, dei dati, né soggetto emittente
Notaio/i *(A5 — da definire)*	Interviene su atto, emissione e liquidazione	Validità/efficacia dell'ancoraggio notarile e riparto di responsabilità da definire
Infrastruttura DLT (registro distribuito)	Ledger su cui operano gli smart contract: **proprietario di JURA Club** (DLT privata/permissioned) **oppure noleggiato da terze parti** (rete pubblica EVM, es. Polygon per l'MVP; o DLT-as-a-service)	Il controllo dell'infrastruttura è di **JURA Club** o del **provider DLT terzo**; **il fornitore tecnico esterno non controlla la DLT**. Modello da confermare (§0.1) — incide su dipendenza da terzi, territorialità e responsabilità
Fornitori terzi (KYC/AML provider, KMS/HSM, hosting)	Sub-fornitori	Eventuali **responsabili/sub-responsabili** del trattamento; DPA a cascata

> Conseguenza metodologica: dove la precedente versione dell'istruttoria riferiva gli obblighi al fornitore, essi vanno **riferiti al Cliente** e alla **sua** giurisdizione. I riferimenti a San Marino restano pertinenti **solo** per la posizione del fornitore tecnico esterno (e per eventuali profili di sub-responsabilità/trasferimento dati verso tale fornitore).

0.1 Scheda Cliente — Dati del Committente

> **Compilata il 2026-07-30** dai dati della visura camerale ordinaria del 24/07/2026. La **sede italiana** del Cliente determina la disciplina applicabile: **MiCAR, GDPR e TUF rilevano in via diretta**; decade l'ipotesi di extraterritorialità per emittente extra-UE.

- **Denominazione sociale: QUANTANA S.R.L.**
- **Forma giuridica:** società a responsabilità limitata — **Società Benefit** (L. 208/2015, commi 376–384)
- **Sede legale:** Via Leopoldo Cerri 9/A, 29122 **Piacenza (PC), Italia** ← *determina la giurisdizione applicabile*
- **Registro delle imprese:** Camera di Commercio dell'**EMILIA** — iscrizione n. **01934410331**, iscritta il 21/07/2026 (sezione ordinaria); **REA PC-373542**
- **Partita IVA / codice fiscale: 01934410331**
- **Legale rappresentante: Alice Luppi**, **Amministratrice Unica** — rappresentanza generale con firma libera, senza limitazioni salvo gli atti eccedenti i limiti statutari
- **Recapiti:** PEC **quantana@pec.it** · altri recapiti (email ordinaria, telefono, indirizzo per comunicazioni legali): [da compilare]
- **Capitale sociale:** 10.000,00 € deliberato, sottoscritto e **interamente versato**
- **Costituzione / durata:** atto del 09/07/2026 · durata al 31/12/2057 · primo esercizio al 31/12/2026
- **Stato attività alla visura: inattiva** (società di nuova costituzione) ⚖ *da verificare l'avvio dell'attività e i codici ATECO prima dell'operatività della piattaforma*
- **DPO / Responsabile protezione dati:** [da compilare / da valutare se obbligatorio] — ⚖ da valutare ex art. 37 GDPR (trattamento su larga scala di dati identità)
- **Rappresentante UE ex art. 27 GDPR: non necessario** — il Cliente è stabilito in uno Stato membro UE
- **Ruolo assunto dal Cliente:** ☑ emittente/promotore ☑ operatore di piattaforma [da confermare formalmente]
- **Dominio/sito della piattaforma:** [da compilare]
- **Infrastruttura DLT:** ☑ noleggiata da terze parti — rete pubblica EVM **Polygon PoS** per l'MVP (D-012) [da confermare]
- **Mercati/giurisdizioni target:** [da compilare] — ⚖ dato ancora mancante e **rilevante**: determina l'eventuale estensione extraterritoriale degli obblighi
- **Legge applicabile e foro** preferiti: [da compilare] — l'orientamento naturale è la legge italiana e il foro della sede, ma va confermato col legale
- **Rapporto con il fornitore tecnico esterno:** proposta economica **OFF-2026-JURACLUB-002** del 30/07/2026 (02_Commerciale/); contratto di sviluppo/fornitura n. [da compilare]; **DPA [da stipulare]**

> ⚠ **Attenzione al profilo Società Benefit.** QUANTANA è costituita come Società Benefit: lo statuto le impone finalità di beneficio comune e una relazione annuale d'impatto. È un elemento che il legale deve considerare, perché incide sull'oggetto sociale perseguibile e sulla rendicontazione — non è un dettaglio formale.

0.2 Scopo del documento e del mandato

Il presente pacchetto fornisce **al legale incaricato dal Cliente** la fattispecie concreta completa della piattaforma JURA Club (predisposta sul piano tecnico dal fornitore tecnico esterno) e formula i **quesiti puntuali** cui si chiede risposta scritta, così da:

1. ottenere il **parere di qualificazione** dei token **JUS** ai sensi del TUF/MiFID II e del Regolamento MiCAR (UE) 2023/1114 — verifica che **sblocca il go-live** (T-002);
2. perimetrare gli **obblighi antiriciclaggio (AML)** e l'eventuale status **CASP/VASP del Cliente**, nella giurisdizione del Cliente e verso i mercati target;
3. impostare la **conformità GDPR** individuando il **Cliente come titolare** e il **fornitore tecnico esterno come responsabile** per i trattamenti svolti per suo conto;
4. validare l'**opponibilità giuridica** dell'adesione ai doveri (privity) e la sua propagazione *pro quota*;
5. raccogliere le **red-line** del legale sui documenti contrattuali/informativi in bozza (T&C, Privacy, Risk Disclaimer, Regole Marketplace, Creator/Buyer Agreement), da emettere **a nome del Cliente**.

---

1. Inquadramento della fattispecie — descrizione tecnica estesa

1.1 Soggetti e prodotto

Il **Cliente** *(§0.1)* è titolare e operatore di **JURA Club**, piattaforma Web3 per l'emissione e la circolazione controllata di **Titoli Digitali Certificati**. È **JURA Club** (la piattaforma operata dal Cliente) a **controllare ed emettere** i Titoli, tramite un'infrastruttura **DLT propria o noleggiata da terze parti** (v. §1.2). Il **fornitore tecnico esterno** ne cura lo **sviluppo tecnico** (software) per conto del Cliente e **non controlla i Titoli né la DLT; il controllo è di JURA Club o del**

provider DLT terzo. Il modello concettuale non tokenizza un mero diritto economico, bensì una **posizione giuridica completa**:

- **JURA** = il titolo, ossia la **posizione giuridica** (proprietà, quota, credito, usufrutto o altra situazione soggettiva) che incorpora **diritti + doveri + limitazioni + condizioni**, **ancorata a un atto notarile** e a un **fascicolo documentale** verificabile;
- **JUS** = la **quota frazionaria fungibile** *pro quota* della JURA. Chi detiene il 30% dei JUS di una data JURA è titolare del 30% dei relativi **diritti e** del 30% dei relativi **doveri**.

Elemento qualificante e distintivo rispetto a un tipico *security token*: il JUS **non incorpora solo un diritto**, ma **anche obblighi e limitazioni opponibili**, condizione tecnica di ricezione della quota (§1.3).

1.2 Standard tecnico e architettura del token

- Standard token: **ERC-1155** (un id per JURA; il balance di quell'id = JUS detenuti) + **modulo di compliance ispirato allo standard ERC-3643** (identità/whitelist e *transfer-restriction*). Evoluzione prevista verso ERC-1400/3643 pieno.
- **Infrastruttura DLT**: il registro distribuito su cui operano gli smart contract è **proprietario di JURA Club** (DLT privata/permissioned) **oppure noleggiato da terze parti** (rete pubblica EVM — es. **Polygon PoS** per l'MVP — o DLT-as-a-service). Il modello (proprietario vs noleggiato) va **confermato** e incide su controllo dell'infrastruttura, dipendenza da terzi, territorialità/localizzazione dei nodi e responsabilità. EVM-compatibile: portabilità tra reti senza riscrittura dei contratti. Scelta soggetta a validazione anche regolamentare.
- **Circolazione permissioned**: solo wallet approvati (KYC) possono ricevere/detenere/trasferire JUS; il gate opera **a livello di token**, non di rete (la rete dell'MVP è pubblica). **Nessun mercato secondario aperto** né quotazione; circolazione **peer-to-peer controllata in whitelist**.

1.3 Gate di ammissibilità: adesione (privity) + KYC

Ogni movimento di JUS (conio, trasferimento) attraversa **due controlli cumulativi** a livello di smart contract, prima dell'esecuzione:

1. **Adesione ai doveri (privity)**: il destinatario deve aver **formalmente accettato on-chain i doveri** della specifica JURA (acceptDuties(id)) prima di ricevere i relativi JUS — presidio volto a rendere gli obblighi **opponibili e propagabili**.

2. **Compliance/KYC**: il destinatario deve risultare **idoneo** (identità verificata, non congelato, eventualmente approvato per l'emissione).

Il trasferimento a soggetto non aderente o non idoneo **è impedito** (revert). Il *burning* (liquidazione) è esente dal gate di adesione.

1.4 Ciclo di vita e ruolo del notaio

- **Emissione/tokenizzazione**: intervento notarile sull'atto; il **fascicolo notarile** è oggetto di **hashing** e il relativo **hash (SHA-256) è ancorato on-chain** (ProofRegistry), con stati di registrazione/validazione/firma. Si definiscono **frazionamento** (totale JUS = 100%) e **scheda diritti/doveri**; quindi conio e allocazione dei JUS ai titolari (aderenti + KYC).
- **Circolazione**: trasferimenti peer-to-peer controllati (gate §1.3), con eventuale *lock-up* per-emissione.
- **Liquidazione/burning**: estinzione della posizione con intervento notarile.

Il **flusso notarile operativo** (notai/partner, tempi, responsabilità) è **decisione ancora aperta lato Cliente (A5)**.

1.5 Separazione dato ↔ prova, vault e accesso ai documenti

- **Principio dato↔prova**: documenti con dati personali **solo off-chain** in **vault cifrato** (**AES-256-GCM**, *envelope encryption*: chiave-dati per-documento avvolta da chiave-master); **on-chain solo l'hash SHA-256** (docRef). Nessun dato personale in chiaro immutabile.
- **Accesso ai documenti**: **gateway** con **autorizzazione a tempo** ("grant a tempo") **tracciata on-chain** (AccessGrant: concessione/scadenza/revoca), per terzi qualificati (notai, avvocati, autorità).
- **Portale di verifica pubblica**: verifica dei **fatti on-chain** di una JURA e dell'**integrità di un documento** via hash calcolato **lato client** (contenuto mai trasmesso). Espone **solo fatti tecnici e integrità**, con disclaimer che *la verifica tecnica non è validazione legale*.

1.6 Identità e wallet

- **KYC obbligatorio per tutti** i titolari; nessun wallet riceve JUS senza approvazione KYC.
- **Wallet ibrido**: **custodial** (chiavi in KMS) e **non-custodial** (SIWE/WalletConnect/MetaMask). *Il modello custodial è il principale trigger di eventuale qualifica CASP/VASP del Cliente e di responsabilità sulla custodia.*

1.7 Perimetro dell'MVP (scelte già assunte, rilevanti per la qualificazione)

- Tipologie ammesse: **basso rischio** — certificati/collezionabili, membership/accessi, utility, crediti documentali.
- **Escluse**: **immobili** e **quote societarie** (voto/dividendi); **moduli finanziari** (stablecoin, collaterale, distribuzione ROI).
- **Nessuna aspettativa di rendimento** promessa; **nessun pooling**; **nessun mercato secondario aperto**.

---

2. Quadro delle decisioni progettuali rilevanti

ID	Decisione	Rilevanza legale
D-005 / D-008	MVP a **basso rischio**; esclusi immobili/quote societarie e moduli finanziari	Fattore mitigante centrale del rischio security token
D-009	**JUS = ERC-1155 + compliance** (ispirato ERC-3643)	Regime di *transfer-restriction*
D-010	**KYC per tutti**; circolazione **permissioned a livello di token**; niente mercato aperto	AML + esclusione offerta indiscriminata
D-011	**Wallet ibrido** custodial + non-custodial	Custodia = possibile trigger CASP/VASP e responsabilità **del Cliente**
D-012	Rete **Polygon PoS** (EVM)	Infrastruttura/ territorialità
D-003 / D-016	**Separazione dato↔prova**	GDPR (minimizzazione, art. 17)
T-022	**Adesione (privity)**	Opponibilità dei doveri (da validare)

A5 (aperta)	**Flusso notarile**	Validità/efficacia dell’ancoraggio

3. Sintesi del rischio già istruita internamente (rif. Allegato B — Memo 01)

Sul piano tecnico e non vincolante è stata condotta una mappatura dei fattori che **aumentano** (aspettativa di ROI; fungibilità/negoziabilità; mercato secondario; offerta a pubblico ampio; diritti societari; promesse di apprezzamento; pooling) e **riducono** (assenza di ROI; doveri/limitazioni; assenza di mercato aperto; KYC/permissioning; tipologie a basso rischio; adesione; ancoraggio a posizione reale) il rischio di qualificazione. Confrontati due scenari (A “basso rischio” — target; B “profilo finanziario” — da evitare). **La qualificazione resta riservata al legale del Cliente.**

---

4. Quesiti al legale (per area) — posti per conto del Cliente

> Per ciascun quesito: **fattispecie rilevante** ed **esito/decisione attesa**. Risposta **scritta e motivata**, con fonti normative e prassi delle autorità competenti **della giurisdizione del Cliente** e dei mercati target.

4.1 Qualificazione degli strumenti (MiFID II / TUF / MiCAR) — *priorità massima, blocca il go-live*

- **Q1.** Nella giurisdizione del Cliente (§0.1) e nei mercati target, i **JUS** delle tipologie MVP sono **strumenti finanziari** (art. 1 TUF / Allegato I MiFID II, o norma equivalente)? La **fungibilità** e il **frazionamento** integrano la **“negoziabilità sul mercato dei capitali”** nonostante l’assenza di mercato aperto e la circolazione solo in whitelist?
- **Q2.** Se non strumenti finanziari, i JUS ricadono in **MiCAR** come **“altro crypto-asset”** (obbligo di **white paper**) o beneficiano di esenzioni? Distinguere per tipologia.
- **Q3.** L’incorporazione di **doveri/limitazioni** e l’**adesione obbligatoria** incidono sulla qualificazione e in che misura allontanano dalla nozione di strumento di investimento?
- **Q4.** Quali **elementi di configurazione o comunicazione** determinerebbero una **riqualificazione**? Fornire una **lista di “linee rosse”** operative.

4.2 Offerta al pubblico e obblighi informativi

- **Q5.** L'emissione/allocazione di JUS costituisce **offerta al pubblico di cripto-attività** (MiCAR)? Quando scatta il **white paper** e quali **esenzioni** valgono (soglie, cerchia ristretta, circolazione limitata alla whitelist)?
- **Q6.** Se il white paper è dovuto: **contenuti minimi**, **notifica** e **autorità competente** (in funzione della sede del Cliente e dei mercati target).

4.3 Territorialità e giurisdizione applicabile

- **Q7.** In funzione della **sede del Cliente** (§0.1) e della platea di utenti target, quale disciplina si applica (UE: MiCAR/TUF diretti; extra-UE con utenti UE: extraterritorialità, necessità di stabilimento/soggetto UE)? È necessario un soggetto/stabilimento in una giurisdizione specifica?
- **Q8.** Sussistono profili di **passporting** o, al contrario, di **divieto di solicitation** che impongano **geoblocking** di determinate giurisdizioni?

4.4 Antiriciclaggio (AML) e status CASP/VASP del Cliente

- **Q9.** Poiché la piattaforma **custodisce** (modello custodial) e **fa circolare** cripto-attività, il **Cliente** assume la qualifica di **CASP/VASP**? Quali **licenze/registrazioni** nella sua giurisdizione e nei mercati target?
- **Q10.** Perimetro AML applicabile al Cliente (adeguata verifica, EDD per PEP/alto rischio, screening **OFAC/UE/ONU**); obbligo di **Travel Rule**?
- **Q11.** Autorità e modalità della **segnalazione di operazioni sospette (SOS)**; **retention** KYC/AML.

4.5 Protezione dei dati (GDPR) — Cliente titolare, fornitore tecnico esterno responsabile

- **Q12.** L'**indirizzo wallet**, pseudonimo ma riconducibile via KYC, è **dato personale**? **Basi giuridiche** (art. 6) dei singoli trattamenti (contratto/adesione; obbligo legale KYC/AML; legittimo interesse)?
- **Q13.** Conferma che il **Cliente è il titolare del trattamento** e il **fornitore tecnico esterno il responsabile (art. 28)** per i trattamenti svolti per suo conto (sviluppo/hosting/manutenzione): quali contenuti minimi del **DPA tra Cliente e fornitore tecnico esterno**? Servono **DPO** e/o **rappresentante UE (art. 27)** in capo al **Cliente** (in funzione della sua sede)? È necessaria una **DPIA**?
- **Q14.** Base giuridica dei **trasferimenti** di dati verso il fornitore tecnico esterno (ove con sede in Paese terzo, es. San Marino) e verso altri sub-fornitori, tenuto conto della sede del Cliente (adeguatezza, SCC, altro).

- **Q15.** È difendibile che il **diritto di cancellazione (art. 17)** si soddisfi cancellando il dato **off-chain**, restando on-chain **solo l'hash** (non reversibile, tesi da validare)? Come conciliare l'**immutabilità dell'audit trail** con la limitazione della conservazione?
- **Q16.** Quali **DPA (art. 28)** deve stipulare il **Cliente** con i fornitori che trattano dati per suo conto (fornitore tecnico esterno, provider KYC, hosting/vault, KMS custodial)?
- **Q31.** Alla luce delle **Linee guida EDPB 02/2025** sul trattamento di dati personali tramite tecnologie blockchain (**versione finale adottata il 7 luglio 2026**): **(a)** l'impianto adottato — **nessun dato personale on-chain**, solo hash SHA-256, contenuto cifrato off-chain — è sufficiente rispetto alle aspettative dell'EDPB, e come va argomentato nella **DPIA**? **(b)** le linee guida invitano a **preferire soluzioni a governance chiusa (permissioned)** e a **motivare** la scelta di modelli più decentralizzati: quale motivazione scritta rende difendibile l'uso di una **rete pubblica** (Polygon PoS) per l'MVP, e quali misure compensative sono attese? **(c)** come si qualificano, in termini di **titolare/responsabile**, i **validatori** della rete pubblica e l'eventuale **provider DLT**? **(d)** l'indirizzo wallet, in quanto dato personale scritto on-chain e non cancellabile, modifica l'impostazione data a Q15?

4.6 Opponibilità dei doveri (privity) — profilo civilistico

- **Q17.** Il meccanismo di **adesione on-chain** (acceptDuties) rende i doveri **opponibili** al titolare e ai **successivi acquirenti**? Quale **forma/contenuto contrattuale** off-chain (a nome del Cliente) è necessario a supporto, inclusa la **propagazione *pro quota*** di diritti e doveri?
- **Q18.** In caso di contestazione dei doveri da parte di un aderente, quali **rimedi** e **clausole** (T&C / Buyer Agreement del Cliente) rafforzano l'opponibilità?

4.7 Fiscalità

- **Q19. Trattamento IVA/imposte** dell'emissione e circolazione dei JUS nella giurisdizione del Cliente e nei mercati target (natura bene/servizio/strumento).
- **Q20.** Obblighi di **reporting cripto (DAC8 / CARF)** in capo al **Cliente**; ritenute/sostituto d'imposta (fermo che l'MVP non prevede ROI/dividendi).

4.8 Tutela del consumatore

- **Q21.** Se i titolari sono **consumatori**: **informazioni precontrattuali** dovute e **diritto di recesso** (vs **irreversibilità** blockchain); invocabilità dell'esclusione per **beni/contenuti digitali su misura**.
- **Q22.** Profili di **vessatorietà** nelle clausole (incluse le limitazioni di responsabilità) dei documenti del Cliente.

4.9 Geoblocking, territorialità, foro

- **Q23.** Quali **giurisdizioni ammesse/escluse** (US persons, Paesi sanzionati, Paesi ostili) e come impostare lo **screening sanzioni** in onboarding.
- **Q24.** Quali **legge applicabile** e **foro competente** indicare nei documenti, coerenti con la **sede del Cliente** e la platea target.

4.10 Proprietà intellettuale

- **Q25.** Titolarità dei **contenuti** del fascicolo e **licenze d'uso** alla piattaforma; **manleva e licenza** per i contenuti dei creator (nei documenti del Cliente).
- **Q26.** Rischi di **anteriorità/omonimia** e opportunità di **registrazione** dei marchi "JURA Club" / "JURA" / "JUS" (a nome del Cliente o del fornitore tecnico esterno, da definire nel rapporto tra Cliente e fornitore tecnico esterno).

4.11 Flusso notarile (A5)

- **Q27. Forma** e **riparto di responsabilità** che rendono valido/efficace l'**ancoraggio notarile** come prova; ruolo del notaio in **emissione** e **liquidazione**.

4.12 Rapporto tra Cliente e fornitore tecnico esterno (profilo contrattuale del progetto)

- **Q28.** Nel contratto di sviluppo/fornitura tra Cliente e fornitore tecnico esterno: ripartizione di **responsabilità** e **manleve** per profili regolamentari (il Cliente come soggetto obbligato; il fornitore tecnico esterno come fornitore), **titolarità del software** e dell'eventuale marchio, **livelli di servizio**, e **DPA** ex art. 28. Quali clausole tutelano il fornitore tecnico esterno dall'assunzione impropria di obblighi da titolare/emittente?

4.13 Infrastruttura DLT (proprietaria vs noleggiata)

- **Q29.** L'infrastruttura DLT su cui gira JURA Club può essere **proprietaria** (DLT privata/permissioned di JURA Club) **oppure noleggiata da terze parti** (rete pubblica EVM come Polygon, o DLT-as-a-service). In che misura tale scelta incide su: (a) **responsabilità e affidamenti** verso il provider DLT (SLA, continuità, exit); (b) **qualificazione e obblighi** connessi all'uso di una rete **pubblica permissionless** vs una **DLT privata permissioned**; (c) **territorialità/localizzazione** dei nodi e dei dati (rilievo GDPR e giurisdizionale); (d) **dipendenza da terzi** e rischio di indisponibilità. Quali **presidi contrattuali** verso il provider DLT (ove noleggiata) e quali cautele (ove proprietaria) sono necessari?

4.14 Registri per la circolazione digitale — Decreto Fintech (Italia)

- **Q30.** Qualora la **disciplina italiana** risulti applicabile (per sede del Cliente o per mercato target) e i **JUS** fossero qualificati come **strumenti finanziari** (Scenario B del memo, Allegato B §5): **(a)** l'emissione e il trasferimento ricadrebbero nell'ambito del **D.L. 25/2023** (conv. **L. 52/2023**, "Decreto Fintech"), in attuazione del **Reg. (UE) 2022/858** *DLT Pilot Regime*, con obbligo di scritturazioni su un **registro per la circolazione digitale**? **(b)** chi potrebbe assumere il ruolo di **responsabile del registro** (soggetto iscritto nell'elenco tenuto da Consob ai sensi del regolamento adottato con **delibera n. 22923 del 7 dicembre 2023**): il Cliente stesso, previa iscrizione, o un soggetto terzo abilitato? **(c)** una **rete pubblica EVM** (Polygon PoS) può integrare un registro per la circolazione digitale, o è tecnicamente e giuridicamente necessaria un'infrastruttura diversa? *In tal caso la deriva verso lo Scenario B comporterebbe un cambio di infrastruttura, non solo obblighi informativi.* **(d)** nello **Scenario A** (JUS non strumenti finanziari) la disciplina resta del tutto inapplicabile, o vi sono profili di attrazione da presidiare in via prudenziale? **(e)** vi sono adempimenti o opportunità connessi al **DLT Pilot Regime** rilevanti per il modello di business del Cliente?

> Questo quesito è stato aggiunto il **2026-07-30** a seguito di un fact check sulle fonti: la disciplina non era richiamata in nessuno degli allegati, pur essendo determinante nello Scenario B e per la scelta di rete (D-012).

---

5. Dati e decisioni che il Cliente deve fornire *(questionario per il Cliente)*

> Compilare per consentire un parere completo. Le risposte confluiscono nei documenti e nell'analisi del legale.

1. **Scheda Cliente (§0.1)** completa (denominazione, sede/Stato, legale rappresentante, P.IVA, PEC…).
2. **Ruolo del Cliente**: emittente, operatore o entrambi.
3. **Mercati/giurisdizioni target** in cui la piattaforma sarà offerta.
4. **Titolare del trattamento** e assetto (contitolari?); nomina **DPO** e **rappresentante UE** se dovuti.
5. **Legge applicabile** e **foro competente** preferiti.
6. **Giurisdizioni ammesse/escluse** (policy geoblocking) e fornitore di **screening sanzioni**.

7. **Provider KYC/KYB** selezionato e livelli di verifica (base/rafforzata, PEP, adverse media).
8. **Notai/partner** del flusso notarile e accordi (chiude A5).
9. **Fornitore KMS/HSM** per la custodia chiavi (modello custodial) e relativi DPA.
10. **Retention** documentale/log (conciliazione GDPR ↔ AML ↔ audit immutabile).
11. **Politiche di comunicazione/marketing** (revisione del copy in ottica *security-token-safe*).
12. **Assetto contrattuale tra Cliente e fornitore tecnico esterno** (contratto di sviluppo, titolarità IP, DPA).

---

6. Allegati da trasmettere al legale

Rif.	Documento	Contenuto
A	00_Compliance_Checklist.md	Checklist compliance con stato per area
B	01_Memo_Qualificazione_Security_Token.md	Memo di rischio (fattori, 2 scenari, presidi)
C	02_Termini_e_Condizioni.md	Bozza T&C (da emettere a nome del Cliente)
D	03_Privacy_Policy.md	Bozza informativa privacy (titolare = Cliente)
E	04_Risk_Disclaimer.md	Bozza disclaimer rischi
F	05_Regole_Marketplace.md	Bozza regole di circolazione
G	06_Creator_Agreement.md / 07_Buyer_Agreement.md	Bozze accordi creator/acquirente
H	08_Cookie_Policy.md	Bozza cookie policy
I	../../01_Architettura/corrente/	Architettura e prodotto (Master Plan)

J	../EVENT_CATALOG.md	Catalogo eventi on-chain (tracciabilità/audit)
K	../PORTAL_API.md	API del portale di verifica pubblica
L	../VAULT_GATEWAY.md	Vault cifrato e gateway con grant a tempo

> Gli allegati tecnici (I–L) descrivono i presidi effettivamente implementati e testati (utili a verificare la coerenza tra dichiarato e realizzato). Nessun parametro proprietario riservato del fornitore tecnico esterno è incluso.

---

7. Deliverable richiesti al legale

1. **Parere scritto e motivato di qualificazione** dei JUS (per tipologia MVP) ex TUF/MiFID II e MiCAR, con **rischio residuo** e conferma della collocazione in "basso rischio" (chiude **T-002**).
2. **Matrice regolamentare** per area (offerta al pubblico/white paper, AML/CASP-VASP, GDPR, consumatore, fiscalità, geoblocking, IP, notarile) → adempimenti, autorità, tempistiche, responsabilità **in capo al Cliente**.
3. **Lista di "linee rosse"** operative.
4. **Red-line e revisione** delle bozze (Allegati C–H), da emettere **a nome del Cliente**.
5. **Piano di rimedi e adempimenti** propedeutici al go-live, con priorità/tempi.
6. **Pareri accessori**: opponibilità della privity (Q17–Q18); tesi GDPR su hash/cancellazione (Q15); assetto tra Cliente e fornitore tecnico esterno (Q28).

---

8. Priorità e sequenza operativa

1. **P0 — Qualificazione (Q1–Q6)**: cancello del **go-live**.
2. **P0 — AML/CASP-VASP (Q9–Q11)** e **GDPR strutturale (Q12–Q16)**.
3. **P1 — Territorialità/geoblocking (Q7–Q8, Q23–Q24)**; **opponibilità privity (Q17–Q18)**; **assetto tra Cliente e fornitore tecnico esterno (Q28)**.
4. **P1 — Revisione documentale (Allegati C–H)** e **fiscalità (Q19–Q20)**.
5. **P2 — Consumatore (Q21–Q22)**, **IP/marchio (Q25–Q26)**, **flusso notarile A5 (Q27)**.

> **Regola di progetto ribadita:** nessuna configurazione tecnica elimina il rischio regolamentare; lo **riduce** e lo rende **difendibile**. Nessun elemento tecnicamente implementato è presentato come legalmente conforme fino alla validazione del legale incaricato dal Cliente.

⚠ Verifiche legali necessarie (rinvio)

Le verifiche di dettaglio sono in coda a ciascun allegato e sintetizzate nella checklist (Allegato A) e nel memo (Allegato B, §7). Il presente pacchetto le **organizza in quesiti** riferiti al **Cliente** e ne definisce **priorità e deliverable**.

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, titolare e operatore della piattaforma JURA Club); da validare con legale abilitato prima di qualsiasi uso. Non costituisce parere legale vincolante. Modello dei ruoli: **titolare del trattamento / operatore / emittente / soggetto obbligato = Cliente**; **fornitore/i tecnico/i esterno/i** (potenziale responsabile del trattamento ex art. 28 per i trattamenti svolti per conto del Cliente). Il Cliente ha sede in **Italia** (Piacenza): la disciplina applicabile è quella **italiana e UE** — MiCAR, GDPR e TUF rilevano in via diretta. San Marino resta rilevante solo come sede del fornitore tecnico esterno (trasferimento dati verso Paese terzo). Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: aggiunte le righe su **Decreto Fintech / registri per la circolazione digitale** (M6), **linee guida EDPB 02/2025** su blockchain e dati personali (G12) e **fiscalità italiana 2026** (F4); corretta la dicitura ambigua sul permissioning, che opera **a livello di token** e non di rete.

00 · Compliance Checklist operativa — JURA Club

0. Scopo e istruzioni d’uso

Checklist di compliance per la piattaforma **JURA Club** (Titoli Digitali Certificati: JURA = titolo/posizione giuridica notarizzata; JUS = quota frazionaria ERC-1155). Copre GDPR, KYC/AML, IP/copyright, fiscalità digitale, MiCA/TUF, tutela del consumatore, geoblocking.

Legenda stato: - ✅ **Presidiato** — misura tecnica implementata e coerente coi fatti di progetto. - 🟡 **Parziale** — impostazione presente, da completare/formalizzare. - ⬜ **Aperto** — da progettare o da decidere (spesso dipendente da validazione legale o da A5). - ⚖ **Verifica legale richiesta** — richiede parere di legale abilitato prima del go-live.

> Nota trasversale: lo stato “tecnicamente implementato” **non** equivale a “legalmente conforme”. Ogni riga ⚖ va chiusa da legale abilitato.

---

1. GDPR / Protezione dati (Reg. UE 2016/679 — applicabile in via diretta: titolare stabilito in Italia)

#	Requisito	Stato	Presidio attuale (fatti progetto)	Da fare / verifica
G1	Minimizzazione dati on-chain	✅	Separazione dato↔prova (D-003/D-016): on-chain solo hash SHA-256 (docRef); nessun dato personale in chiaro immutabile	Confermare che nessun evento/log on-chain contenga dati personali indiretti (indirizzi wallet = dato personale, vedi G2)
G2	Qualificazione indirizzo wallet come dato personale	⚖	Wallet ibrido (D-011); KYC lega wallet↔identità	⚖ Indirizzo wallet pseudonimizzato ma riconducibile → **dato personale**. Definire base giuridica e informativa dedicata

G3	Cifratura documenti off-chain		AES-256-GCM in vault, AAD=docRef anti-swap (D-016/D-017)	Gestione chiavi via KMS/HSM in produzione (residuo T-023)
G4	Basi giuridiche del trattamento	⚖	Contratto (adesione/privity), obbligo legale (KYC/AML)	⚖ Mappare ogni trattamento alla base ex art. 6 (contratto / obbligo legale / legittimo interesse); vedi 03_Privacy_Policy
G5	Titolare del trattamento	⚖	**Cliente** (**QUANTANA S.R.L.**) titolare del trattamento; il/i fornitore/i tecnico/i esterno/i responsabile/i ex art. 28 per i trattamenti svolti per suo conto	⚖ **Da definire in capo al Cliente**: eventuali contitolari e **DPO** (art. 37, da valutare). Il **rappresentante UE ex art. 27 non serve**: QUANTANA è stabilita in Italia
G6	Trasferimenti di dati verso Paesi terzi (dipende dalla sede del Cliente; incl. verso	⚖	Valutazione in funzione della **sede del Cliente**; il fornitore tecnico esterno con	⚖ **Da definire** base per i trasferimenti (adeguatezza, SCC) rispetto alla sede del Cliente e

	fornitore/i tecnico/i esterno/i con sede in Paese terzo, es. San Marino, come sub-responsabile)		sede in Paese terzo (es. San Marino) è sub-responsabile/destinatario dei dati per sviluppo/hosting	verso il/i fornitore/i tecnico/i esterno/i in Paese terzo; rilevante se utenti UE
G7	Diritti dell’interessato vs immutabilità blockchain	⚖	Cancellazione: solo off-chain; on-chain resta hash non reversibile	⚖ Documentare che l’hash non è dato personale e che la cancellazione off-chain “svuota” la prova; validare tesi
G8	Conservazione log e audit		AuditTrail on-chain (immutabile) + grant a tempo tracciati	Definire retention dei log off-chain; conciliare immutabilità audit con limitazione conservazione
G9	DPIA (valutazione d’impatto)	⚖	—	⚖ **Necessaria**: trattamento su larga scala + tecnologia innovativa + dati identità (KYC)
G10	Registro dei trattamenti (art. 30)		—	Da redigere

G11	Nomina responsabili (art. 28)	⚖	Provider KYC, vault/hosting, custodial wallet KMS; **fornitore/i tecnico/i esterno/i** quale responsabile per sviluppo/hosting/manutenzione	⚖ DPA che il **Cliente** (titolare) stipula con ogni responsabile che tratta dati per suo conto, **incluso il/i fornitore/i tecnico/i esterno/i**
G12	Linee guida **EDPB 02/2025** su blockchain e dati personali (versione finale adottata il **7 luglio 2026**)	⚖	L'architettura è già allineata al principio centrale: **nessun dato personale on-chain**, solo hash; contenuto cifrato off-chain (D-003/D-016)	⚖ Argomentare **esplicitamente** l'allineamento nella DPIA (G9) e nella privacy policy. Due punti da chiudere: (a) l'EDPB invita a **preferire blockchain a governance chiusa** e a **motivare** la scelta di modelli più decentralizzati → serve la motivazione scritta della scelta di **Polygon PoS**, rete pubblica (D-012); (b) ruoli

				titolare/responsabile rispetto ai validatori e al provider DLT

2. KYC / AML — Antiriciclaggio

#	Requisito	Stato	Presidio	Da fare / verifica
A1	KYC obbligatorio per tutti i titolari		D-010: nessun wallet riceve JUS senza KYC-approval; gate pre-trasferimento (T-022)	—
A2	Whitelist dei titolari (permissioning **a livello di token**)		Solo wallet approvati detengono/trasferiscono JUS: whitelist KYC nel registro di compliance + gate nel trasferimento (D-010). **La rete resta pubblica** (Polygon PoS, D-012): il controllo è applicativo, non di rete	Mantenere la distinzione in ogni documento: un gate di token non equivale a una rete chiusa
A3	Quadro AML applicabile	⚖	Perimetro in funzione della **sede del**	⚖ **Da definire** il perimetro AML:

			Cliente e dei mercati target; utenti potenzialmente UE/IT	normativa **italiana** (d.lgs. 231/2007 e successive modifiche) + **MiCAR/AMLR UE** ove il Cliente sia qualificato CASP; obblighi Travel Rule
A4	Qualificazione come VASP/CASP	⚖	Piattaforma custodisce (custodial) e trasferisce cripto-attività	⚖ Verificare se il **Cliente** è **prestatore di servizi per le cripto-attività (CASP)** ai sensi di MiCAR → autorizzazione e vigilanza **Consob/Banca d'Italia**
A5	Adeguata verifica rafforzata (PEP, alto rischio)		Provider KYC da selezionare	Definire livelli KYC/KYB, screening sanzioni, PEP, adverse media
A6	Segnalazione operazioni sospette (SOS)	⚖	—	⚖ Procedura SOS verso l'**UIF — Unità di Informazione Finanziaria per l'Italia** (Banca

				d’Italia), competente per la sede del Cliente
A7	Conservazione dati KYC		Vault cifrato	Retention AML (tipicamente 5–10 anni) da fissare con G8

3. IP / Copyright

#	Requisito	Stato	Presidio	Da fare / verifica
I1	Titolarità contenuti del fascicolo documentale	⚖	Fascicolo notarile off-chain	⚖ Chiarire diritti su atti/perizie/allegati caricati; licenza d’uso alla piattaforma
I2	Diritti su marchio “JURA Club” / “JURA” / “JUS”	⚖	Brand identity v1.0	⚖ Verifica anteriorità e registrazione marchio (rischio omonimie in ambito legal-tech)
I3	Licenze software / dipendenze (software di base riuso)		Software di base del fornitore tecnico esterno (titolare del software di base, con	Verificare compatibilità licenze OSS; il software di base è IP del fornitore tecnico esterno (no

			licenza d’uso a JURA Club); OZ e librerie OSS	VVT esposto)
I4	Contenuti caricati dai creator	⚖	—	⚖ Clausole di manleva e licenza nei Creator Agreement (06)

4. Fiscalità digitale

#	Requisito	Stato	Presidio	Da fare / verifica
F1	Trattamento IVA/imposte su emissione e circolazione JUS	⚖	—	⚖ **Da definire** con fiscalista: natura del JUS (bene/servizio/ strumento) ai fini IVA nella giurisdizione del **Cliente** e nei mercati target
F2	Obblighi di reporting cripto (DAC8 / CARF)	⚖	—	⚖ Verificare applicabilità DAC8/CARF al **Cliente** come possibile reporting provider
F3	Ritenute e sostituto d’imposta	⚖	—	⚖ Da valutare in base a natura dei flussi (nessun ROI/dividendo

				nell’MVP, D-005)
F4	Quadro fiscale italiano vigente (contesto, se il Cliente o i mercati target sono IT)	⚖	—	⚖ Dato di contesto al 2026-07-30, **non** una qualificazione: sulle plusvalenze e sui proventi da **cripto-attività** realizzati **dal 1° gennaio 2026** si applica l’aliquota del **33%**, con mantenimento del **26%** per le **stablecoin ancorate all’euro**; la soglia di esenzione di 2.000 € è **abolita dal 1° gennaio 2025**. Resta da stabilire con fiscalista **se i JUS siano “cripto-attività”** ai fini fiscali: dipende dalla qualificazione di T-002

5. MiCA / TUF — Rischio strumento finanziario (CENTRALE)

#	Requisito	Stato	Presidio	Da fare / verifica
M1	Qualificazione JUS (security token?)	⚖	Architettura MVP a basso rischio (D-005/D-008): no ROI, no mercato aperto, doveri on-chain	⚖ **Parere T-002** — vedi 01_Memo_Qualificazione_Security_Token
M2	Esclusione asset finanziari dall'MVP		Esclusi immobili e quote societarie (voto/dividendi); moduli finanziari ArgonX fuori perimetro (D-005)	Mantenere il perimetro; ogni ampliamento → nuova valutazione
M3	Assenza mercato secondario aperto		Circolazione ammessa solo fra titolari in whitelist KYC (permissioning a livello di token, D-010); nessuna quotazione né exchange aperto	Regole circolazione in 05_Regole_Marketplace. ⚖ Nota: il gate è applicativo, la rete sottostante è pubblica — argomento da presentare con precisione nel test di negoziabilità
M4	Qualificazione MiCA	⚖	JUS non è stablecoin	⚖ Se non strumento

	(ART/EMT/altro crypto-asset)			finanziario, valutare se “altro crypto-asset” MiCA → obbligo white paper
M5	White paper / offerta al pubblico	⚖	—	⚖ Verificare se emissione JUS = offerta al pubblico di cripto-attività
M6	**Decreto Fintech** — emissione su registro per la circolazione digitale (scenario “strumento finanziario”)	⚖	Nessun presidio: oggi l’emissione avviene su rete pubblica EVM, senza responsabile del registro	⚖ **Da verificare**: se i JUS fossero qualificati come strumenti finanziari e la disciplina italiana risultasse applicabile (sede del Cliente o mercato target IT), l’emissione e il trasferimento dovrebbero avvenire tramite scritturazioni su un **registro per la circolazione digitale** tenuto da un **responsabile**

				del registro iscritto nell’elenco Consob (D.L. 25/2023 conv. L. 52/2023, in attuazione del Reg. UE 2022/858; regolamento Consob adottato con delibera n. 22923 del 7-12-2023). Incide direttamente sulla scelta di rete (D-012) e sul quesito Q29

6. Tutela del consumatore

#	Requisito	Stato	Presidio	Da fare / verifica
C1	Informazioni precontrattuali	⚖	T&C + Risk Disclaimer (02,04)	⚖ Verificare completezza vs Codice del Consumo IT / dir. UE se utenti consumatori
C2	Diritto di recesso	⚖	Irreversibilità blockchain confligge con recesso	⚖ Chiarire se/quando si applica; eventuale esclusione per beni digitali

				su misura
C3	Clausole vessatorie	⚖	—	⚖ Revisione clausole T&C per squilibrio
C4	Trasparenza costi/gas	⚠	Polygon PoS = gas minimi (D-012)	Esplicitare costi e chi li sostiene

7. Geoblocking / Territorialità

#	Requisito	Stato	Presidio	Da fare / verifica
T1	Paesi ammessi / esclusi	⚖	La whitelist KYC a livello di token consente il filtro per titolare	⚖ **Da definire** whitelist/black list giurisdizioni (US persons, Paesi sanzionati, Paesi a normativa cripto ostile)
T2	Screening sanzioni (OFAC/UE/ONU)	⚠	Gate KYC	Integrare screening liste sanzioni in onboarding
T3	Legge applicabile e foro	⚖	Da definire in base alla **sede del Cliente**	⚖ **Da definire** giurisdizione competente e foro nei T&C, coerenti con la sede del Cliente e la platea target

⚠ Verifiche legali necessarie (sintesi prioritaria)

1. **T-002 — Qualificazione JUS** come strumento finanziario/security token (MiCA + TUF): parere scritto (vedi 01). *Blocca il go-live.*
2. **Perimetro AML e status VASP/CASP** del **Cliente** (in funzione della sua sede e dei mercati target): licenze, Travel Rule, SOS.
3. **Titolare del trattamento (= Cliente), DPIA, trasferimenti verso Paesi terzi** (in funzione della sede del Cliente e verso il/i fornitore/i tecnico/i esterno/i con sede in Paese terzo, es. San Marino, come sub-responsabile) e qualificazione wallet come dato personale.
4. **Giurisdizione, foro competente, legge applicabile** (dato mancante — "da definire").
5. **Geoblocking**: giurisdizioni ammesse/escluse e screening sanzioni.
6. **Fiscalità** (IVA, DAC8/CARF, aliquote applicabili) su emissione e circolazione JUS — vedi F4.
7. **A5 flusso notarile** (aperto lato cliente): responsabilità e validità legale dell'ancoraggio notarile.
8. **Decreto Fintech / registro per la circolazione digitale** (M6): applicabilità nello scenario "strumento finanziario" e individuazione del responsabile del registro. *Incide sulla scelta di rete.*
9. **EDPB 02/2025** (G12): motivazione scritta della scelta di una rete pubblica anziché di una DLT chiusa, e ruoli privacy rispetto a validatori e provider DLT.

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Non costituisce parere legale vincolante né consulenza in materia di servizi di investimento. Supporto tecnico predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, soggetto emittente/operatore della piattaforma), per istruire il parere T-002; **da emettere/utilizzare a nome del Cliente previa validazione legale**. La qualificazione resta riservata al legale incaricato dal Cliente. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: aggiunta la conseguenza infrastrutturale dello Scenario B (Decreto Fintech, registri per la circolazione digitale) e precisato che il permissioning opera a livello di token.

01 · Memo — Rischio di qualificazione dei JUS come strumenti finanziari / security token (MiCA · TUF)

1. Oggetto e limiti del memo

Analisi **tecnico-preparatoria** del rischio che le quote **JUS** (ERC-1155; id = JURA, balance = JUS) siano qualificate come **strumenti finanziari** (art. 1 TUF / MiFID II) o rientrino nell'ambito di **MiCAR (Reg. UE 2023/1114)** in modo da attivare obblighi di prospetto/white paper, autorizzazione e vigilanza.

Questo memo **non decide** la qualificazione: la qualificazione è un giudizio giuridico riservato a legale abilitato (T-002). Serve a (a) mappare i fattori di rischio, (b) mostrare come l'architettura JURA li incide, (c) elencare le verifiche legali.

> Il rischio "security token" è il **rischio centrale** dichiarato del progetto (D-005). Va minimizzato e sempre segnalato.

2. Cosa è (e cosa non è) un JUS — inquadramento fattuale

- Il token JURA porta on-chain una **posizione giuridica completa**: diritti **+ doveri + limitazioni + condizioni**, ancorata a atto notarile e fascicolo documentale.
- Il **JUS** è la quota frazionaria *pro quota* di quella posizione. Chi detiene il 30% dei JUS detiene il 30% dei diritti **e** dei doveri.
- Presupposto tecnico per ricevere JUS: **adesione ai doveri** (privity, T-022) + **KYC** (D-010). **Circolazione permissioned**: solo titolari in whitelist KYC possono ricevere JUS, con gate **a livello di token** su rete pubblica (Polygon PoS, D-012). **Nessun mercato secondario aperto**.

Elemento distintivo rispetto a un tipico security token: il JUS **non incorpora solo un diritto economico**, ma anche **doveri e limitazioni** — è più vicino a un "titolo di partecipazione a una posizione giuridica" che a un mero strumento di investimento. Questo è un argomento a favore del basso rischio, **ma non è di per sé dirimente**.

3. Fattori che AUMENTANO il rischio (profilo "strumento finanziario")

#	Fattore	Perché aumenta	Presente in

		il rischio	JURA?
R1	Aspettativa di **rendimento/ROI** dall'altrui attività	Cuore del test di strumento finanziario/investment contract	**No** nell'MVP (D-005) — da presidiare
R2	**Fungibilità** e negoziabilità del token	Negoziabilità sul mercato dei capitali = indice di valore mobiliare	JUS **fungibile pro quota** → attenzione
R3	**Mercato secondario** liquido/aperto	Negoziabilità = requisito valore mobiliare	**No** — circolazione ammessa solo in whitelist (gate a livello di token), nessun exchange (D-010)
R4	Frazionamento e distribuzione a **pubblico ampio**	Offerta al pubblico → prospetto/white paper	Frazionamento **sì**; pubblico limitato da KYC/permissioning
R5	Diritti tipici societari (**voto, dividendi**)	Assimilazione ad azioni/quote	**Esclusi** dall'MVP (immobili e quote societarie fuori, D-005)
R6	Promesse di **apprezzamento** in comunicazione/marketing	Riqualificazione di fatto a prodotto d'investimento	**Da presidiare** nel copy (lessico security-token-safe)
R7	**Pooling** di fondi con gestione centralizzata	Schemi di investimento collettivo	Da evitare/segnalare

4. Fattori che RIDUCONO il rischio (architettura JURA)

#	Fattore	Effetto mitigante	Fonte progetto
M1	**Nessun ROI atteso** dall'MVP	Manca l'elemento "aspettativa di profitto da altrui attività"	D-005/D-008
M2	**Doveri e limitazioni** on-chain (non solo diritti)	Il token non è puro strumento di investimento; incorpora obblighi	D-001, GLOSSARIO
M3	**Nessun mercato secondario aperto**	Non "negoziabile sul mercato dei capitali"	D-010
M4	**KYC obbligatorio + permissioning**	Circolazione controllata, non offerta indiscriminata al pubblico	D-010
M5	**Tipologie a basso rischio** (certificati, membership, utility, crediti documentali)	Esclusi immobili/quote societarie e moduli finanziari	D-005/D-008
M6	**Adesione (privity)** come condizione	Rafforza natura "posizione giuridica" vs strumento fungibile astratto	T-022
M7	**Ancoraggio notarile** a posizione reale	Il token è certificato di una posizione, non promessa finanziaria	D-003, A5 (aperto)

5. Due scenari a confronto

Scenario A — “Basso rischio” (target MVP)

- **Configurazione:** certificati/membership/utility/crediti documentali; nessun ROI; nessun voto/dividendo; circolazione permissioned in whitelist (a livello di token); KYC per tutti; nessun mercato aperto; copy privo di promesse di rendimento.
- **Esito atteso (ipotesi, da validare):** JUS con maggior probabilità **fuori** dal perimetro “strumento finanziario” TUF; da verificare se rientra in MiCAR come “**altro crypto-asset**” (che comporterebbe comunque un **white paper** MiCA, non un prospetto).
- **Rischio residuo:** la **fungibilità** (R2) e il **frazionamento** (R4) restano indici da neutralizzare tramite permissioning e assenza di mercato. Riqualificazione possibile se la comunicazione veicola aspettative di guadagno (R6).
- **Presidi raccomandati:** vedi §6.

Scenario B — “Profilo finanziario” (da evitare, mostrato per contrasto)

- **Configurazione:** JUS liberamente trasferibili su mercato secondario, con aspettativa di apprezzamento, riferiti a immobili/quote societarie con diritti economici (dividendi) o rendimenti da gestione.
- **Esito atteso (ipotesi):** alta probabilità di qualificazione come **strumento finanziario/security token** → TUF (offerta al pubblico, prospetto, autorizzazioni MiFID) e/o regime security fuori MiCA.
- **Conseguenze:** obblighi autorizzativi pesanti, vigilanza, responsabilità; incompatibile con un MVP snello.
- **Conseguenza ulteriore, spesso trascurata — infrastruttura di emissione (Italia).** Se la disciplina italiana risultasse applicabile (sede del Cliente o mercato target IT), lo Scenario B non comporterebbe soltanto obblighi informativi e autorizzativi: l’emissione e il trasferimento di **strumenti finanziari digitali** devono avvenire tramite scritturazioni su un **registro per la circolazione digitale**, tenuto da un **responsabile del registro** iscritto in un elenco tenuto da Consob (**D.L. 25/2023**, conv. **L. 52/2023** — “Decreto Fintech” —, in attuazione del **Reg. (UE) 2022/858** *DLT Pilot Regime*; regolamento attuativo Consob adottato con **delibera
    n. 22923 del 7 dicembre 2023**). Ne discende che, in Scenario B,** una rete pubblica EVM non è di per sé un registro per la circolazione digitale** e occorrerebbe individuare chi ne sia il responsabile: la deriva verso B non è quindi solo un aggravio documentale, ma un **cambio di**

infrastruttura. ⚖ *Applicabilità e conseguenze da verificare col legale — vedi Q30 in 09.*

> **Raccomandazione:** mantenere rigorosamente lo Scenario A; trattare qualsiasi deriva verso B come **decisione regolamentata** da non assumere senza parere e presidio autorizzativo.

6. Presidi raccomandati (per restare in Scenario A)

1. **Perimetro prodotto blindato**: nessun diritto di voto/dividendo, nessun immobile/quota societaria nell'MVP (mantenere D-005).
2. **Nessuna promessa di rendimento**: lessico security-token-safe in tutti i materiali; disclaimer coerenti (04_Risk_Disclaimer).
3. **Permissioning + KYC** come barriera all'offerta indiscriminata (D-010).
4. **Nessun mercato secondario aperto**; circolazione solo peer-to-peer controllata in whitelist (05_Regole_Marketplace).
5. **Doveri effettivi e opponibili** (privity) documentati — rafforzano la natura non meramente finanziaria; ma l'**opponibilità giuridica** dell'adesione va validata (T-022 lato legale).
6. **Governance del perimetro**: ogni nuova tipologia di JURA passa da una valutazione di qualificazione prima del rilascio.
7. **Documentazione a supporto** (questo memo + parere T-002) agli atti prima del go-live.

7. Rischio regolamentare — dichiarazione

Anche nello Scenario A, **residua incertezza**: la qualificazione dipende da fatti concreti (comunicazione, effettiva circolazione, diritti reali incorporati) e dall'evoluzione di MiCAR e delle prassi delle **autorità competenti della giurisdizione del Cliente** e dei mercati target (a titolo esemplificativo, per utenti IT/UE: CONSOB/Banca d'Italia). Nessuna configurazione tecnica elimina il rischio: lo **riduce** e lo rende **difendibile**.

⚠ Verifiche legali necessarie

1. **Parere scritto T-002** sulla qualificazione dei JUS (tipologie MVP) come strumenti finanziari ex TUF/MiFID II e sul loro inquadramento MiCAR (strumento finanziario escluso da MiCA vs "altro crypto-asset" soggetto a white paper). *Blocca il go-live.*

2. **Test dell'offerta al pubblico**: se e quando l'emissione/allocazione di JUS costituisca offerta al pubblico di cripto-attività → obblighi informativi (white paper MiCA) o esenzioni.
3. **Giurisdizione applicabile**: individuazione della disciplina in funzione della **sede del Cliente** (emittente/operatore) e dei mercati target; se il Cliente è UE → MiCAR/TUF in via diretta; se extra-UE con utenti UE → analisi di extraterritorialità. Coordinamento con l'eventuale posizione del fornitore tecnico esterno come mero fornitore tecnologico.
4. **Opponibilità giuridica dell'adesione (privity)** e dei doveri pro-quota (interazione con T-022).
5. **Impatto della fungibilità/frazionamento** sui test di negoziabilità: se i presidi di permissioning bastano a escludere la "negoziabilità sul mercato dei capitali". Da valutare con precisione il fatto che il permissioning opera **a livello di token** e non di rete: la rete sottostante (Polygon PoS) è pubblica e permissionless.
6. **Decreto Fintech / registri per la circolazione digitale**: se la disciplina italiana è applicabile, verificare gli obblighi infrastrutturali in Scenario B (registro, responsabile del registro iscritto in elenco Consob) e l'eventuale rilevanza del **DLT Pilot Regime**. Vedi Q30 in 09_Pacchetto_Consegna_Legale.
7. **Validazione del copy** marketing/commerciale (assenza di elementi che veicolino aspettativa di rendimento — R6).

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Testo-base non vincolante. Numerosi campi sono "da definire" (giurisdizione, foro, dati del Cliente). Da completare e validare con legale abilitato. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, gestore della piattaforma e controparte contrattuale dell'utente); da validare con legale abilitato prima di qualsiasi uso. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: corretta la definizione di permissioning (a livello di token, non di rete).

02 · Termini e Condizioni d’uso — JURA Club

1. Premesse e definizioni

JURA Club è una piattaforma Web3 per l’emissione, la certificazione e la circolazione controllata di **Titoli Digitali Certificati** (“JURA”). Gestore e titolare della piattaforma, nonché controparte contrattuale dell’utente: ****QUANTANA S.R.L.**** (“Piattaforma”, “Gestore”). La piattaforma è sviluppata e mantenuta, per conto del Gestore, da un **fornitore tecnico esterno** (titolare del software di base, con licenza d’uso a JURA Club), che **non è parte** del presente contratto né titolare dei rapporti con l’utente.

- **JURA** — Titolo digitale certificato: rappresentazione on-chain di una posizione giuridica (diritti, doveri, limitazioni, condizioni) ancorata a un atto notarile e a un fascicolo documentale verificabile.
- **JUS** — Quota frazionaria fungibile *pro quota* di una JURA (standard ERC-1155; id = JURA, balance = JUS). Chi detiene una quota di JUS detiene la corrispondente quota di **diritti e doveri**.
- **Adesione (privity)** — Accettazione formale dei doveri, condizione tecnica e giuridica per ricevere JUS.
- **Titolare** — Utente KYC-verificato che detiene JUS.
- **Creator / Emittente** — Soggetto che promuove l’emissione di una JURA.
- **Circolazione permissioned** — Regime in cui solo wallet approvati (whitelist, KYC) possono detenere/trasferire JUS. Il controllo è applicativo, **a livello di token**: la rete sottostante è pubblica.

2. Natura del token e assenza di natura finanziaria

2.1 Il JUS rappresenta una **quota di una posizione giuridica** certificata, comprensiva di **doveri e limitazioni**, e **non** è emesso né offerto come strumento finanziario, prodotto d’investimento o titolo di partecipazione societaria.

2.2 Nell’ambito operativo attuale (MVP) sono **esclusi**: diritti di voto societario, dividendi, rendimenti garantiti, immobili e quote societarie. La Piattaforma **non promette alcun rendimento** e non garantisce apprezzamento di valore.

2.3 ⚖ *La qualificazione giuridica del JUS è oggetto di valutazione legale (vedi 01_Memo e 04_Risk_Disclaimer). Questa clausola descrive l’intento del Gestore, non una qualificazione certa.*

3. Requisiti di accesso

3.1 **KYC obbligatorio per tutti**: nessun utente può ricevere/detenere JUS senza verifica dell'identità approvata (circolazione permissioned in whitelist).

3.2 L'utente dichiara di non risiedere in giurisdizioni escluse (**da definire** in sede di geoblocking) e di non essere soggetto a misure restrittive/sanzioni.

3.3 **Adesione ai doveri**: prima di ricevere JUS l'utente accetta on-chain i doveri associati alla JURA. Senza adesione, il trasferimento è tecnicamente bloccato.

4. Wallet e custodia delle chiavi

4.1 La Piattaforma supporta wallet **custodial** (chiavi gestite dal Gestore via KMS) e **non-custodial** (chiavi in controllo esclusivo dell'utente).

4.2 Nel modello **non-custodial** l'utente è **unico responsabile** della custodia delle chiavi: la loro perdita comporta la **perdita irreversibile** dell'accesso ai JUS. La Piattaforma non può recuperarle.

4.3 Nel modello **custodial** il Gestore adotta misure di sicurezza ma **non offre garanzie** oltre quanto previsto dalla legge applicabile.

5. Ruoli e responsabilità

5.1 Piattaforma / Gestore

- Fornisce l'infrastruttura tecnica (smart contract, vault, indexer) "così com'è".
- **Non è parte** dei rapporti giuridici sottostanti tra creator e titolari, salvo diversa indicazione.
- Non garantisce la veridicità dei contenuti caricati dai creator (fascicolo documentale), fatti salvi i controlli descritti.
- ⚖ Ruolo del Gestore rispetto all'ancoraggio notarile: **da definire** (A5, flusso notarile aperto).

5.2 Creator / Emittente

- Risponde della **veridicità, legittimità e completezza** dei documenti e della posizione giuridica rappresentata dalla JURA.
- Garantisce la titolarità o i diritti sui contenuti caricati e manleva la Piattaforma (vedi 06_Creator_Agreement).

5.3 Titolare / Acquirente

- È responsabile della propria idoneità (KYC, giurisdizione), della custodia chiavi (§4) e del rispetto dei **doveri** assunti con l'adesione.
- Riconosce l'**irreversibilità** delle operazioni on-chain.

6. Rischi (rinvio)

L'utente dichiara di aver letto e compreso il **04_Risk_Disclaimer** (rischi tecnologici, regolamentari, di irreversibilità e di custodia). L'uso della Piattaforma implica l'accettazione di tali rischi.

7. Limitazioni di responsabilità

7.1 Nei limiti massimi consentiti dalla legge applicabile, il Gestore non risponde di: malfunzionamenti della blockchain Polygon PoS o di terze reti, perdita di chiavi, azioni di terzi, oscillazioni di valore, riqualificazioni normative sopravvenute.

7.2 ⚖ *Le clausole di esonero/limitazione vanno verificate rispetto a norme imperative (tutela consumatore, clausole vessatorie).*

8. Condotte vietate e blocco wallet

Sono vietati: uso per riciclaggio/finanziamento del terrorismo, elusione del KYC, caricamento di contenuti illeciti o lesivi di IP altrui. Il Gestore può **sospendere/bloccare wallet o JUS segnalati** secondo le 05_Regole_Marketplace.

9. Proprietà intellettuale

I diritti su software, marchi ("JURA Club", "JURA", "JUS") e contenuti della Piattaforma restano del Gestore. I creator concedono le licenze necessarie all'erogazione del servizio (dettaglio in 06).

10. Modifiche, sospensione, cessazione

Il Gestore può aggiornare i presenti T&C e sospendere il servizio per manutenzione/sicurezza/obblighi legali, con informativa agli utenti secondo modalità **da definire**.

11. Legge applicabile e foro

⚖ **Da definire in base alla sede del Cliente** (Gestore): legge applicabile e **foro competente**; regime specifico per utenti consumatori UE/IT. Non forzare San Marino: San Marino rileva solo per la posizione del fornitore tecnico esterno.

12. Trattamento dei dati

Il trattamento dei dati personali è disciplinato dalla **03_Privacy_Policy**, che costituisce parte integrante.

⚠ Verifiche legali necessarie

1. **Qualificazione del JUS** (§2) da allineare al parere T-002; non presentare la natura non-finanziaria come certa.
2. **Legge applicabile e foro** (§11) — dato mancante, da definire.
3. **Titolare/gestore dei rapporti** e ruolo rispetto all'ancoraggio notarile (A5 aperto).
4. **Limitazioni di responsabilità e clausole vessatorie** (§7) vs tutela del consumatore.
5. **Diritto di recesso** vs irreversibilità blockchain (non trattato qui, rinvio a checklist C2).
6. **Requisiti precontrattuali** e forma di accettazione (click-wrap) validi nell'ordinamento competente.

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza di informativa privacy. Titolare (= Cliente), DPO, basi giuridiche e trasferimenti sono da confermare con legale abilitato. Non usare prima della validazione. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, titolare del trattamento); da validare con legale abilitato prima di qualsiasi uso. Il/i **fornitore/i tecnico/i esterno/i** è/sono **responsabile/i del trattamento ex art. 28** per i soli trattamenti svolti per conto del Cliente (sviluppo/hosting/manutenzione), da disciplinare con **DPA**. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: aggiunto il riquadro

> sulle Linee guida EDPB 02/2025 (versione finale 7 luglio 2026) e i due profili aperti da chiudere.

03 · Privacy Policy (GDPR) — JURA Club

1. Titolare del trattamento

Titolare del trattamento: ****QUANTANA S.R.L.**** (denominazione, sede/Stato, recapiti, PEC), operatore e titolare della piattaforma JURA Club.

⚖ **Da definire/confermare in capo al Cliente**: eventuali contitolari e **DPO** (art. 37, da valutare: trattamento su larga scala di dati identità). Il **rappresentante UE ex art. 27 non è necessario**, perché il titolare è stabilito in **Italia**.

Responsabile del trattamento (art. 28): il/i **fornitore/i tecnico/i esterno/i** (responsabile del trattamento ex art. 28), da disciplinare con **DPA**, per i soli trattamenti svolti per conto del Cliente (sviluppo, hosting, manutenzione). Il fornitore tecnico esterno **non** è titolare del trattamento.

2. Categorie di dati trattati

Categoria	Esempi	Fonte
Dati identificativi (KYC)	Nome, documento, dati anagrafici, verifica identità	Onboarding (obbligatorio per tutti, D-010)
Dati wallet	Indirizzo wallet on-chain, saldi JUS, storico transazioni	Piattaforma / blockchain
Dati del fascicolo documentale	Documenti, atti, perizie (possibili dati personali di terzi)	Caricamento creator, off-chain cifrato
Dati tecnici/log	Log di accesso, audit trail, grant a tempo	Uso della Piattaforma

Nota sull’indirizzo wallet: sebbene pseudonimo, se collegato all’identità KYC è **dato personale**. Sulla blockchain resta pubblico e non cancellabile.

3. Separazione dato ↔ prova (impianto tecnico)

- I **documenti** (con eventuali dati personali) risiedono **solo off-chain**, in vault **cifrato AES-256-GCM** (D-003/D-016).
- **On-chain** vive **solo l'hash SHA-256** del documento (docRef): non rivela il contenuto e non costituisce dato personale in chiaro.
- Conseguenza: la **cancellazione** avviene off-chain; l'hash on-chain resta ma, privato del documento, **non consente di risalire ai dati**. ⚖ *Tesi da validare legalmente (art. 17 vs immutabilità).*

> **Linee guida EDPB 02/2025 — blockchain e dati personali** (versione finale adottata il **7 luglio 2026**). L'impianto descritto sopra è stato progettato secondo il principio che le linee guida pongono al centro: **evitare la memorizzazione di dati personali sulla blockchain**, conservandoli off-chain e ancorando on-chain il solo elemento di prova. Restano due profili aperti, che il **Cliente** deve chiudere con il proprio legale prima del go-live: **(a)** le linee guida invitano a **preferire soluzioni a governance chiusa (permissioned)** e a **motivare** la scelta di modelli più decentralizzati — la scelta di una **rete pubblica** (Polygon PoS) per l'MVP va quindi motivata per iscritto, indicando le misure compensative; **(b)** la qualificazione dei **validatori** della rete e dell'eventuale **provider DLT** in termini di titolare/responsabile del trattamento. Si segnala inoltre che l'**indirizzo wallet**, scritto on-chain e non cancellabile, è ragionevolmente **dato personale** (§2): il presidio della separazione dato↔prova non lo copre. ⚖ *Vedi quesito Q31 in 09_Pacchetto_Consegna_Legale e riga G12 della checklist.*

4. Finalità e basi giuridiche (art. 6)

Finalità	Base giuridica (proposta)	Note
Verifica identità (KYC)	Obbligo legale (AML) e/o esecuzione del contratto	⚖ dipende da perimetro AML (checklist §2)
Emissione/gestione JUS, adesione ai doveri	Esecuzione del contratto	Privity/adesione
Sicurezza, audit, prevenzione abusi	Legittimo interesse / obbligo legale	Bilanciamento da documentare
Comunicazioni di servizio	Esecuzione del contratto	—
Marketing (eventuale)	Consenso	Solo se attivato

⚖ *Ogni base giuridica va confermata dal legale; l’elenco è preliminare.*

5. Conservazione dei dati (retention)

- **Dati KYC/AML**: conservazione per il periodo imposto dalla normativa antiriciclaggio applicabile (**da definire**, tipicamente 5–10 anni).
- **Log e audit trail**: l’AuditTrail on-chain è **immutabile**; i log off-chain hanno retention da definire, conciliando immutabilità e principio di limitazione.
- **Documenti del fascicolo**: per la durata della posizione giuridica + periodi legali; poi cancellazione off-chain.

6. Diritti dell’interessato (artt. 15–22)

Accesso, rettifica, cancellazione, limitazione, opposizione, portabilità. Limiti pratici: - **Cancellazione**: eseguibile off-chain; l’hash on-chain non è cancellabile ma è reso inintelligibile dalla rimozione del documento. - **Dati wallet on-chain**: pubblici e non modificabili/cancellabili sulla blockchain.

⚖ *L’informativa deve spiegare chiaramente questi limiti tecnici all’interessato.*

7. Destinatari e responsabili del trattamento

- Il/i **fornitore/i tecnico/i esterno/i** quale **responsabile ex art. 28** per sviluppo/hosting/manutenzione; **provider KYC/AML**, **hosting/vault**, **KMS custodial**, eventuale **notaio/partner** (A5, da definire) quali ulteriori responsabili/sub-responsabili.
- Il **Cliente (titolare)** stipula con ciascuno un **accordo ex art. 28** (DPA), incluso quello con il/i fornitore/i tecnico/i esterno/i. ⚖ *Da predisporre.*

8. Trasferimenti extra-UE

Il titolare è stabilito in **Italia**: il GDPR si applica in via diretta e i trasferimenti rilevanti sono quelli **in uscita** verso Paesi terzi. In particolare il **fornitore tecnico esterno ha sede in San Marino**, Paese terzo rispetto alla UE: per i dati ivi trasferiti (sviluppo, hosting, manutenzione) occorre individuare la base del trasferimento. ⚖ **Da definire**: verificare l’applicabilità di una decisione di adeguatezza per San Marino e, in mancanza, adottare **clausole contrattuali tipo**

(SCC) con valutazione d’impatto sul trasferimento; analoga valutazione per ogni altro sub-responsabile fuori UE.

9. Misure di sicurezza

Cifratura at-rest (AES-256-GCM), AAD anti-swap legato al docRef (D-017), accesso ai documenti solo tramite **grant a tempo** revocabile e tracciato, permissioning e KYC. Gestione chiavi via **KMS/HSM** in produzione (residuo T-023).

10. Processo decisionale automatizzato

Il gating dei trasferimenti (KYC/adesione) è basato su regole deterministiche on-chain. ⚖ *Valutare se costituisce trattamento automatizzato rilevante ex art. 22.*

⚠ Verifiche legali necessarie

1. **Titolare (= Cliente) / contitolari, DPO, rappresentante UE (art. 27)** in capo al Cliente — dati mancanti, da definire in funzione della sede del Cliente.
2. **DPIA** obbligatoria (larga scala + tecnologia innovativa + dati identità).
3. **Trasferimenti verso Paesi terzi** (in funzione della sede del Cliente; in particolare verso il/i fornitore/i tecnico/i esterno/i con sede in Paese terzo, es. San Marino, come responsabile/sub-responsabile): base giuridica del trasferimento.
4. **Qualificazione dell’indirizzo wallet** come dato personale e informativa dedicata.
5. **Conciliazione art. 17 (cancellazione)** con l’immutabilità di hash e audit on-chain: validare la tesi della §3/§6.
6. **Retention** KYC/AML e log: durate esatte.
7. **DPA** che il Cliente (titolare) stipula con tutti i responsabili (**fornitore/i tecnico/i esterno/i**, KYC, vault, KMS, notaio).

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza di informativa sui rischi. Da validare con legale abilitato e allineare al parere T-002 prima di ogni uso. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, Gestore della piattaforma); da validare con legale abilitato prima di qualsiasi uso. “Gestore” nel testo indica il Cliente. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del

> placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: corretta la dicitura sul permissioning.

04 · Risk Disclaimer — JURA Club

> **Avvertenza.** L'uso di JURA Club comporta rischi. Leggi attentamente prima di ricevere o detenere JUS. Se non comprendi i rischi, non procedere e consulta un professionista.

1. Rischio tecnologico (blockchain)

1.1 I JUS vivono su **Polygon PoS** (rete EVM di terze parti). La Piattaforma **non controlla** la rete: congestioni, aumenti di gas, fork, malfunzionamenti, riorganizzazioni di blocchi o interruzioni possono incidere su disponibilità e operatività.

1.2 Gli **smart contract** possono contenere vulnerabilità nonostante test e audit. Un audit esterno pre-mainnet è previsto (T-050) ma **nessun software è privo di rischi**.

1.3 Dipendenze da componenti off-chain (vault, indexer, gateway): disservizi possono limitare l'accesso ai documenti o alla visualizzazione dello stato.

2. Irreversibilità delle operazioni

2.1 Le transazioni on-chain sono **definitive e irreversibili**. Un trasferimento errato di JUS, verso un indirizzo sbagliato o non voluto, **non può essere annullato** dalla Piattaforma.

2.2 L'emissione, l'allocazione e il burning dei JUS producono effetti permanenti sul registro.

3. Rischio di custodia delle chiavi

3.1 **Wallet non-custodial**: l'utente è **unico responsabile** della custodia delle chiavi private/seed. La loro perdita o compromissione comporta la **perdita irreversibile** dei JUS. La Piattaforma **non può recuperarle**.

3.2 **Wallet custodial**: il Gestore custodisce le chiavi con misure di sicurezza (KMS/HSM), ma permangono rischi di sicurezza informatica; nessuna garanzia oltre quanto previsto dalla legge.

4. Rischio regolamentare (CENTRALE)

4.1 Il quadro normativo su cripto-attività (a titolo esemplificativo **MiCAR** UE, **TUF** IT, e la normativa applicabile in funzione della **sede del Cliente** e dei mercati target, AML) è in **evoluzione**. Interpretazioni o modifiche future potrebbero incidere sulla qualificazione dei JUS, sull'operatività o sulla liceità di alcune funzioni.

4.2 ⚖ **Qualificazione come strumento finanziario/security token**: la Piattaforma progetta i JUS per **restare a basso rischio regolamentare** (no ROI, no mercato aperto, doveri on-chain, KYC, esclusione di immobili/quote societarie). **Tuttavia il rischio non è azzerato** e la qualificazione definitiva è oggetto di valutazione legale (T-002). L'utente accetta questo rischio residuo.

4.3 **Nessuna promessa di rendimento**: i JUS non sono offerti come investimento; il Gestore non garantisce alcun profitto né apprezzamento di valore.

5. Rischio di valore e liquidità

5.1 Non esiste un **mercato secondario aperto** (circolazione permissioned in whitelist): la possibilità di trasferire i JUS è **limitata** e subordinata a KYC e adesione della controparte.

5.2 Il valore di una posizione può variare ed è legato alla **posizione giuridica sottostante** e ai relativi **doveri**, non solo ai diritti.

6. Rischio giuridico sui doveri (privity)

6.1 Ricevere JUS implica **assumere doveri e limitazioni** pro-quota. ⚖ L'**opponibilità e la propagazione** di tali doveri sono meccanismi tecnici (adesione on-chain, T-022) la cui **efficacia giuridica è in corso di validazione** legale.

7. Rischio sul fascicolo documentale e ancoraggio notarile

7.1 L'integrità del documento è garantita dall'hash on-chain, ma la **veridicità e legittimità** dei contenuti dipendono dal creator/emittente e dal processo notarile.

7.2 ⚖ Il **flusso notarile** (partner/notai, responsabilità) è ancora **da definire** (A5): fino alla sua chiusura, l'efficacia probatoria dell'ancoraggio non è garantita.

8. Rischio di terzi e sicurezza

Phishing, compromissione di dispositivi, frodi e attacchi a fornitori terzi possono compromettere l'accesso o i fondi. L'utente adotta misure di sicurezza adeguate.

⚠ Verifiche legali necessarie

1. Allineare §4 al **parere T-002** (qualificazione) e alla checklist MiCA/TUF.
2. Validare la formulazione dell'**accettazione del rischio residuo** (efficacia come esonero).
3. Validare §6 sull'**opponibilità dei doveri** (T-022).
4. Coordinare §7 con la **chiusura di A5** (flusso notarile).
5. Verificare compatibilità dei disclaimer con la **tutela del consumatore** (limiti agli esoneri).

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza di regole di circolazione in regime permissioned (whitelist a livello di token). Da validare con legale abilitato; alcune scelte dipendono da A5 e dal parere T-002. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, Gestore/operatore della piattaforma); da validare con legale abilitato prima di qualsiasi uso. "Gestore" nel testo indica il Cliente. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: corretta la dicitura sul permissioning (gate a livello di token su rete pubblica).

05 · Regole del Marketplace / Circolazione dei JUS — JURA Club

> Nota di posizionamento: JURA Club **non è un exchange** né un mercato secondario aperto. È un ambiente di **circolazione controllata** (permissioned) di quote JUS tra soggetti verificati. Questa scelta è un presidio anti-security-token (vedi 01_Memo).

1. Principi generali

1.1 **Circolazione permissioned**: solo wallet approvati (whitelist, KYC) possono detenere e trasferire JUS (D-010). Il gate opera **a livello di token**; la rete sottostante è pubblica (D-012).

1.2 **Nessun mercato secondario aperto**, nessun order book pubblico, nessuna quotazione. I trasferimenti sono **peer-to-peer controllati**.

1.3 Ogni trasferimento è subordinato a **due gate on-chain**: - **Adesione (privity)**: il destinatario deve aver accettato i **doveri** della JURA (T-022); - **Compliance KYC**: il destinatario deve essere KYC-approvato (registro di compliance riusato da ArgonX).

Se uno dei due gate non è soddisfatto, il trasferimento è **tecnicamente bloccato** (chokepoint _update).

2. Condizioni per trasferire JUS

Requisito	Descrizione
KYC mittente e destinatario	Entrambi verificati e non sospesi
Adesione destinatario	Accettazione doveri pro-quota della JURA
Giurisdizione ammessa	⚖ **Da definire** whitelist/blacklist Paesi (geoblocking)
Assenza da liste sanzioni	Screening OFAC/UE/ONU (da integrare)
Assenza di blocchi/segnalazioni	Wallet e JUS non sospesi (§4)

3. Frazionamento e limiti

3.1 Il frazionamento è definito da JuraSubdivision (cap = totale JUS, emittente, lock-up). Il conio JUS è controllato (gate adesione + KYC + cap).

3.2 ⚖ Eventuali **limiti per titolare** (concentrazione massima, soglie) sono post-MVP (T-030) e possono avere rilievo regolamentare (evitare profili di offerta al pubblico) — da valutare.

4. Blocco e sospensione di wallet / JUS segnalati

4.1 Il Gestore può **sospendere o bloccare** wallet o specifici JUS in caso di: sospetto riciclaggio, esito negativo su liste sanzioni, ordine dell'autorità, contenuti illeciti nel fascicolo, violazione dei T&C.

4.2 Il blocco opera tramite gli strumenti di compliance del token (revoca whitelist / freeze). ⚖ *Basi giuridiche e procedura di blocco/ripristino da validare (giusto processo, diritti dell'utente).*

5. Gestione delle dispute

5.1 Controversie sulla **posizione giuridica sottostante** (validità dei diritti/doveri, veridicità del fascicolo) sono estranee alla mera infrastruttura tecnica e ricadono sul **creator/emittente** e sul processo notarile (A5).

5.2 Controversie **tecniche** (trasferimenti, accessi, gating): il Gestore (Cliente), avvalendosi del fornitore tecnologico, fornisce supporto e log/audit trail come evidenza. ⚖ *Meccanismo di risoluzione (reclami, ODR, arbitrato/foro) da definire con la clausola di legge applicabile (02 §11), coerente con la sede del Cliente.*

5.3 Data l'**irreversibilità** on-chain, la Piattaforma non può annullare trasferimenti; può solo agire con gli strumenti di compliance (§4) per operazioni future.

6. Ancoraggio notarile e circolazione

⚖ La circolazione presuppone che la posizione giuridica sia validamente ancorata (atto notarile + fascicolo). Fino alla **chiusura di A5** (flusso notarile: notai, tempi, responsabilità), le regole di questo capitolo restano **provvisorie** per la parte notarile.

7. Tracciabilità e trasparenza

Ogni evento rilevante (emissione, allocazione, adesione, trasferimento, blocco) è indicizzato (indexer read-only, EVENT_CATALOG) e verificabile, nel rispetto della privacy (dati personali off-chain, on-chain solo hash).

⚠ Verifiche legali necessarie

1. **Geoblocking**: whitelist/blacklist giurisdizioni e screening sanzioni (§2, §4).

2. **Basi giuridiche e procedura di blocco** wallet/JUS: giusto processo, tutela dell'utente (§4).
3. **Assenza di mercato secondario** confermata come presidio anti-security-token (coordinare con T-002).
4. **Meccanismo dispute e legge applicabile/foro** (§5) — dato mancante.
5. **Chiusura A5** (flusso notarile) per completare §6.
6. **Limiti per titolare** e loro rilievo regolamentare (§3.2).

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza sintetica. Da validare con legale abilitato. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, gestore della piattaforma e parte dell'accordo); da validare con legale abilitato prima di qualsiasi uso. Il fornitore tecnico esterno non è parte del rapporto con il Creator. Versione: v0.2 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.2: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta.

06 · Creator / Emittente Agreement — JURA Club (bozza sintetica)

1. Oggetto

Accordo tra ****QUANTANA S.R.L.**** (gestore e titolare della piattaforma, di seguito "Piattaforma") e il **Creator/Emittente** che promuove l'emissione di una **JURA** (Titolo Digitale Certificato) e la relativa frazionabilità in **JUS**.

2. Dichiarazioni e garanzie del Creator

- Titolarità o legittimazione sulla **posizione giuridica** rappresentata e sui **contenuti** del fascicolo documentale.
- **Veridicità, legittimità e completezza** di atti, perizie e allegati caricati.
- Rispetto della normativa applicabile (IP, AML, protezione dati di terzi presenti nei documenti).
- Nessuna offerta come strumento finanziario/investimento; nessuna promessa di rendimento (coerenza con 01_Memo e 04_Risk_Disclaimer).

3. Licenze

Il Creator concede alla Piattaforma le licenze necessarie a erogare il servizio (archiviazione cifrata, ancoraggio hash, visualizzazione controllata), senza trasferimento di proprietà dei contenuti.

4. Obblighi di compliance

- Fornire i dati per KYC/KYB del Creator.
- Collaborare al processo notarile e al caricamento del fascicolo. ⚖ Ruoli/responsabilità notarili **da definire** (A5).
- Definizione chiara dei **doveri** associati alla JURA che i titolari assumono con l'adesione (privity).

5. Responsabilità e manleva

Il Creator **manleva** la Piattaforma da pretese di terzi derivanti da falsità/illegittimità dei contenuti o della posizione giuridica, nei limiti di legge.

6. Corrispettivi

⚖ **Da definire**: fee di emissione, modello economico, trattamento fiscale (checklist §4).

7. Durata, sospensione, cessazione

La Piattaforma può sospendere l'emissione in caso di violazione, ordine dell'autorità o rischio legale/regolamentare.

8. Legge applicabile e foro

⚖ **Da definire in base alla sede del Cliente** (coordinare con 02 §11); non forzare San Marino.

⚠ Verifiche legali necessarie

1. Riparto di **responsabilità** Creator/Piattaforma e validità della **manleva**.
2. Ruolo del Creator nel **flusso notarile** (A5 aperto).

3. **Modello economico e fiscalità** delle fee.
4. Qualificazione dell’operazione (evitare profilo di **offerta al pubblico** — T-002).
5. Legge applicabile e foro.

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza sintetica. Da validare con legale abilitato. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, gestore della piattaforma e controparte contrattuale del Titolare); da validare con legale abilitato prima di qualsiasi uso. Il fornitore tecnico esterno non è parte del rapporto con il Titolare. Versione: v0.3 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.3: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta. Novità v0.2: corretta la dicitura sul permissioning.

07 · Buyer / Titolare Agreement — JURA Club (bozza sintetica)

1. Oggetto

Condizioni, poste da ****QUANTANA S.R.L.**** (gestore e titolare della piattaforma), per l’acquisizione e la detenzione di **JUS** (quote frazionarie di una JURA) da parte di un **Titolare** verificato.

2. Requisiti del Titolare

- **KYC obbligatorio** approvato (D-010); wallet ammesso alla whitelist dei titolari.
- **Adesione ai doveri** (privity, T-022) della JURA prima di ricevere JUS.
- Residenza in **giurisdizione ammessa** (⚖ geoblocking da definire) e assenza da liste sanzioni.

3. Natura di ciò che si acquisisce

- Il Titolare acquisisce una **quota pro-quota** di una **posizione giuridica** comprensiva di **diritti E doveri e limitazioni** — **non** uno strumento finanziario né un investimento con rendimento atteso.

- ⚖ La qualificazione giuridica è oggetto di valutazione legale (T-002); nessuna certezza è garantita.

4. Rischi accettati

Il Titolare dichiara di aver letto e compreso il **04_Risk_Disclaimer**: irreversibilità, custodia chiavi, rischio tecnologico e **rischio regolamentare residuo**.

5. Doveri assunti

Con l'adesione, il Titolare assume i **doveri** pro-quota associati alla JURA. ⚖ L'opponibilità di tali doveri è in corso di validazione legale.

6. Trasferimento dei JUS

Consentito solo verso destinatari **KYC + aderenti**; nessun mercato secondario aperto (05_Regole_Marketplace). I trasferimenti sono **irreversibili**.

7. Trattamento dati

Disciplinato dalla **03_Privacy_Policy**.

8. Legge applicabile e foro

⚖ **Da definire in base alla sede del Cliente**; regime specifico se il Titolare è **consumatore** UE/IT. Non forzare San Marino.

⚠ Verifiche legali necessarie

1. **Natura del token** (§3) allineata a T-002; non presentarla come certa.
2. **Opponibilità dei doveri** al Titolare (§5, T-022).
3. **Tutela del consumatore** (recesso, clausole vessatorie) se acquirente consumatore.
4. **Geoblocking** e sanzioni (§2).
5. Legge applicabile e foro.

> **BOZZA — documento tecnico-preparatorio, NON parere legale. Da validare con legale abilitato prima di qualsiasi uso.** Bozza sintetica.

> Presuppone accertamento tecnico dei cookie effettivamente usati. Da validare con legale abilitato. Documento predisposto per **JURA Club** (società titolare: **QUANTANA S.R.L.**, titolare del sito/app e del trattamento); da validare con legale abilitato prima di qualsiasi uso. Versione: v0.2 · Data: 2026-07-30 · Stato: DRAFT interno Novità v0.2: inserito il committente reale **QUANTANA S.R.L.** (visura 24/07/2026) al posto del placeholder; aggiornate le formulazioni che dipendevano dalla sede del Cliente, ora nota: **Italia** → MiCAR, GDPR e TUF in via diretta.

08 · Cookie Policy — JURA Club (bozza sintetica)

1. Premessa

Questa policy descrive l'uso di cookie e tecnologie analoghe sul sito/app JURA Club. ⚖ **Da completare** dopo l'accertamento tecnico dei cookie effettivamente impiegati (audit cookie).

2. Categorie

Categoria	Finalità	Base giuridica	Consenso
Tecnici/necessari	Funzionamento, sicurezza, sessione, connessione wallet	Legittimo interesse / necessità tecnica	Non richiesto
Preferenze	Lingua, impostazioni UI	Consenso (se non strettamente necessari)	Sì
Analitici	Statistiche d'uso	Consenso (salvo analytics anonimizzati)	Sì
Marketing/terze parti	Profilazione	Consenso	Sì

⚖ *La classificazione va confermata sui cookie reali.*

3. Gestione del consenso

Banner cookie con opzioni granulari (accetta/rifiuta/personalizza), registrazione del consenso e possibilità di revoca. ⚖ Conformità a GDPR/ePrivacy (e prassi Garante IT se utenti IT) da verificare.

4. Cookie di terze parti

Provider KYC, eventuali strumenti analitici/CDN: da elencare con relative informative. ⚖ Verificare trasferimenti extra-UE (coordinare con 03 §8).

5. Durata e aggiornamenti

Durata per cookie (da specificare); la policy può essere aggiornata con avviso.

⚠ Verifiche legali necessarie

1. **Audit tecnico dei cookie** reali e completamento tabella §2.
2. Conformità **ePrivacy/GDPR** del banner e della registrazione del consenso.
3. **Cookie di terze parti** e trasferimenti extra-UE.
4. Coordinamento con 03_Privacy_Policy e con il **regime applicabile in funzione della sede del Cliente** (titolare) e dei mercati target.