Cookies and technical tools

Service terms and information. The customer’s executed agreement, order, and schedules govern.

OOKIE AND TECHNICAL STORAGE POLICY (COOKIE POLICY)

Service Provider (Data Controller): DEXIMA TECH LLC, 5830 E 2nd St, Ste 7000 #32263, Casper, Wyoming 82609, USA

Effective Date: 01/2026 - Last Updated: 11/2026

Privacy and DPO Contact: privacy@loricai.io This Cookie Policy constitutes an integral part of the Global Privacy &

Data Protection Policy ("Privacy Policy" - Section 5) and the Terms of Service ("ToS") of the LoricAI platform.

1. "PRIVACY-BY-DESIGN" APPROACH AND ABSOLUTE ABSENCE OF PROFILING
In accordance with Section 5 of the Privacy Policy (Negative Covenants), DEXIMA TECH LLC adopts a strict Privacy-by-Design approach (Art. 25 GDPR). The official website and the LoricAI platform are engineered to operate without any profiling cookies, advertising tracking, cross-site marketing, or third-party behavioral analytics. We do not use Google Analytics, Meta Pixel (Facebook), session-replay software (e.g., Hotjar), advertising fingerprinting, or similar covert tracking technologies.

2. REGULATORY FRAMEWORK AND CONSENT BANNER EXEMPTION (ePRIVACY DIRECTIVE AND SUPERVISORY AUTHORITY GUIDELINES)
Pursuant to Article 5(3) of Directive 2002/58/EC (ePrivacy Directive), Article 122 of Italian Legislative Decree 196/2003 (Italian Privacy Code), the Guidelines on cookies and other tracking tools issued by the Italian Data Protection Authority (Provision no. 231 of June 10, 2021), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and the guidelines of the European Data Protection Board (EDPB), the cookies and local storage tools used by LoricAI fall exclusively within the category of strictly necessary technical tools: (a) to carry out the transmission of a communication over an electronic communications network and to protect the infrastructure against cyberattacks (Art. 6(1)(f) and Recital 49 of the GDPR); (b) to provide the Service explicitly requested by the User, maintain the authenticated session, and enable on-device cryptographic operations (Art. 6(1)(b) of the GDPR). Because only strictly necessary technical cookies and identifiers are used, applicable law does not require obtaining the User's prior consent nor displaying a blocking consent banner (Cookie Wall). The Company fully discharges its transparency information obligation (Art. 13 GDPR) through the publication of this document.

3. DETAILS OF TECHNICAL TOOLS AND SECURITY COOKIES USED
Below is a description of the technical cookies and browser local storage tools (Web Storage / localStorage / sessionStorage) employed on the public portal, in the Dashboard, and in the payment modules of LoricAI: 1. Authentication, Session, and On-Device Encryption (First-Party - LoricAI) Identifiers / Storage: auth_token (HttpOnly, Secure, SameSite Cookie), JWT (JSON Web Token) session tokens, and technical browser local memory (localStorage / sessionStorage). Technical Purpose and Legal Basis: Maintaining the User's authenticated session in the Dashboard, storing the interface language preference (IT, EN, DE, FR, ES), verifying AMD/NVIDIA Remote Attestation, and locally managing on-device encryption (Cryptographic Client Module) prior to transmission to the hardware enclave in Finland (Performance of a contract - Art. 6.1.b GDPR).

Duration / Persistence: Proprietary authentication tokens are limited in duration to the active Session and are invalidated upon logout or session closure; technical interface preferences persist locally in the browser until deleted by the User. 2. Perimeter Network Security and DDoS Mitigation (Sub-Processor - Cloudflare, Inc.) Identifiers: __cf_bm, cf_clearance (and equivalent Web Application Firewall / Bot Management technical cookies). Technical Purpose and Legal Basis: Distinguishing between legitimate human traffic and malicious automated traffic (bots), perimeter protection against volumetric attacks (DDoS), and network infrastructure security, without any behavioral profiling or cross-site tracking purpose (Legitimate interest in network security - Art. 6.1.f and Recital 49 GDPR). Duration / Persistence: __cf_bm expires after 30 minutes of inactivity; cf_clearance (where triggered by a network security check) has a technical duration of up to a maximum of 30 minutes / verification session.

3. Electronic Payment Fraud Prevention (Payment Gateways - Stripe / PayPal) Identifiers: __stripe_mid, __stripe_sid (set by Stripe Payments Europe Ltd.) and technical session/anti-fraud cookies of PayPal (Europe) S.à r.l. et Cie, S.C.A. Technical Purpose and Legal Basis: Activated exclusively in the subscription and electronic payment sections to ensure the security of financial transactions (PCI-DSS SAQ A compliance) and prevent payment fraud (Performance of a contract and statutory anti-money laundering/anti-fraud obligations - Arts. 6.1.b and 6.1.c GDPR). Such tools are completely isolated from document workspaces and have no access whatsoever to Payload Data. Duration / Persistence: __stripe_sid lasts 30 minutes (payment session); __stripe_mid lasts 1 year for anti-fraud recognition of the payment device.

4. MANAGEMENT OF BROWSER SETTINGS AND TECHNICAL IMPACT ON THE SERVICE
The User may at any time inspect, restrict, or delete cookies and local storage data (localStorage / sessionStorage) through the security settings of their browser (Chrome, Firefox, Safari, Edge, Brave).
However, because LoricAI uses such elements exclusively for secure authentication, on-device encryption, and WAF perimeter protection, blocking technical cookies or browser local storage altogether will make it technically impossible to log into the Dashboard, verify the enclave's cryptographic attestation, and access encrypted workspaces until technical permissions are restored in the browser.

5. DATA SUBJECT RIGHTS AND REFERENCE TO THE PRIVACY POLICY
For all information regarding privacy roles (Data Controller and Data Processor under Art. 28 GDPR), international transfer safeguards (Standard Contractual Clauses SCCs and Sub-Processors' Data Privacy Framework DPF certifications), governing law and exclusive jurisdiction (Article 8 of the ToS and Section 10 of the Privacy Policy), as well as to exercise at any time the rights provided under Articles 15-22 of the GDPR, the User may consult the Global Privacy & Data Protection Policy or contact the Privacy & Compliance Department at: privacy@loricai.io.