LEGAL / TECHNICAL

Written authorization for penetration test

Aligned with KZ-1 Art. 221, GDPR Art. 28, ZVOP-2; NIST SP 800-115 and PTES framework.

/ 1 — PARTIES

This authorization is entered into between:

Client (system controller)

Full legal name	_____
Registry number	_____
Tax ID	_____
Address	_____
Statutory representative	_____
Title	_____
Email / phone	_____

Provider (processor)

Full legal name	Računalničar, Sebastijan Bandur s.p.
Registry number	8839883000
Tax ID	68283270
Address	Marjeta na Dravskem polju 39, 2206 Marjeta na Dravskem polju, Slovenija
Statutory representative	Sebastijan Bandur
Email	sebastijan.bandur.sp@gmail.com
Website	racunalnicar.eu
IBAN / bank	SI56 1010 0005 9138 955 (Banka Intesa Sanpaolo d.d.)
VAT-liable	No (ZDDV-1 Art. 94)

/ 2 — SCOPE

The Provider is authorized to perform a penetration test on the targets listed below. Any system or address not explicitly listed is out of scope.

IP / CIDR (e.g. 203.0.113.0/24)	_____
	_____
URLs / applications	_____
	_____
	_____
User populations (roles, test accounts)	_____
Specific API endpoints	_____

EXPLICITLY OUT OF SCOPE

The following test types are NOT permitted without a separate written authorization: production databases, third-party systems (host, CDN, payment processor), social engineering (phishing, vishing), denial-of-service attacks (DoS/DDoS), physical testing, access to the hosting provider's management interfaces.

/ 3 — TIME WINDOW

Start date	____ / ____ / 2026
End date	____ / ____ / 2026
Permitted hours	passive: 0–24h · invasive: ____ – ____
Time zone	Europe/Ljubljana (CET/CEST)

/ 4 — SOURCE-IP ALLOWLIST

The Client will allowlist the Provider's source IPs in its own WAF / SIEM / firewall for the duration of the test. The Provider declares the following IPs:

IPv4 / IPv6 (CIDR) _____

_____

/ 5 — DATA PROCESSING (GDPR ART. 28) + NDA

If the pentest touches personal data, processor terms under GDPR Art. 28 apply. The Provider undertakes to:
(a) process personal data only on the Client's documented instructions;
(b) ensure personnel and sub-processors are under written confidentiality;
(c) implement appropriate technical and organizational measures (GDPR Art. 32);
(d) not engage sub-processors without prior written consent;
(e) assist the Client in responding to data-subject requests;
(f) assist the Client in compliance with GDPR Arts. 32–36;
(g) at the end of the service, return or delete personal data (Client's choice);
(h) make available all information necessary to demonstrate Art. 28(3)(h) compliance.

Confidentiality (NDA): Provider does not disclose data to third parties, encrypts data at rest and in transit, and stores data within the EU.

/ 6 — REPORTING + EVIDENCE RETENTION

Report recipient (name, email)	_____
Report format	PDF (report) + JSON (evidence)
Raw evidence retention	12 months (encrypted, Provider only)
Final report retention	5 years (OZ — Slovenian Code of Obligations)
Destruction method	cryptographic erasure (key destruction)

/ 7 — CRITICAL-FINDING ESCALATION

For findings with CVSS ≥ 9.0 or actively exploitable vulnerabilities, the Provider notifies the Client within the time stated, via the channels stated.

Primary contact	_____
24/7 phone	_____
Secondary contact	_____
Notification window	4 hours from discovery
Notification channel	call + encrypted email

/ 8 — LEGAL + TECHNICAL FRAMEWORK

Legal framework: KZ-1 Art. 221 (Attack on Information System), Art. 143 (Abuse of Personal Data), Art. 220 (Damage to Another's Property) · GDPR Art. 6(1)(f), Recital 49, Art. 28 · ZVOP-2 (Official Gazette RS 163/22) · OZ (Code of Obligations) · ZEPT Art. 7 (validity of electronic form).

Technical framework: OWASP ASVS 5.0.0 (May 2025) · OWASP Top 10:2025 · PTES (Pre-engagement → Reporting) · NIST SP 800-115 · MITRE ATT&CK v19 (April 2026) · CVSS v4.0 (with v3.1 secondary) · CWE 4.20.

ASVS level	L1 / L2 / L3 (circle one)
Top 10:2025 coverage	A01–A10 (all) / selected: _____
PTES phases	PE · IG · TM · VA · EX · PE2 · RP

/ 9 — LIABILITY + LIMITS

System ownership: the Client warrants legal authority over all systems in scope. If a system is on shared hosting (e.g., SI host, Cloudflare, AWS), the Client attaches a separate written permission from the host or confirms the test is within the provider's published policy. For managed CMS (WordPress.com, Wix, Squarespace, managed Shopify), testing is not permitted without the provider's explicit consent.

Provider liability: Provider acts as a professional processor; liability is limited to direct damage caused by intent or gross negligence, up to the value of the engagement, except where mandatory law (personal data, death, serious bodily injury) requires otherwise.

/ 10 — SIGNATURES

This authorization takes effect on handwritten signature by both parties, or on qualified electronic signature (eIDAS / SI-PASS / SI-TRUST). Original or signed PDF.

Client (statutory representative)	Provider
_____	_____
name	Sebastijan Bandur · Računalničar, Sebastijan Bandur s.p.
_____	_____
signature · place · date	signature · Marjeta na Dravskem polju · date

Template · v.2026.06 · racunalnicar.eu/docs/written-authorization.pdf · changes follow PISRS and ip-rs.si