BlackProtect Comprehensive Terms of Service & Legal Framework

Bilingual Legal Specification (German / English): Terms of Service (TOS), Acceptable Use Policy (AUP), Service Specifications & Liability Privileges for Beta/Production

Dokumenten-ID / Version:	BP-LEG-2026-V2.1 (Bilingual Dual-Language Edition)
Geltungsbereich / Scope:	blackprotect.net, bp.tuerkmen.dev (Dashboards, Edge-Nodes, eBPF/XDP-Module, APIs, Attack Simulator)
Betreiber / Provider:	BlackProtect Platform (Inhaber: Muhammed Ali Türkmen / tuerkmen.dev)
Rechtsstatus / Legal Status:	Kostenlose Beta- & Evaluierungsphase (Public Showcase) sowie gewerbliche Vorschriften

Sonderregelung zur Beta- & Testphase / Special Notice regarding Beta Phase (§ 521 BGB):

Soweit die Dienste von BlackProtect dem Kunden im Rahmen der Beta- oder Showcase-Phase unentgeltlich überlassen werden, haftet der Anbieter gemäß § 521 BGB gesetzlich beschränkt ausschließlich für Vorsatz und grobe Fahrlässigkeit. Es bestehen keinerlei Garantien hinsichtlich Verfügbarkeit oder SLA.
To the extent BlackProtect services are provided free of charge during the beta or showcase phase, liability is limited under § 521 BGB strictly to intent and gross negligence. No guarantees or SLAs regarding uptime or latency are provided.

TEIL I: ALLGEMEINE GESCHÄFTSBEDINGUNGEN (DEUTSCH)

§ 1 Geltungsbereich, Rangfolge & Vertragssprache

(1) Diese Allgemeinen Geschäftsbedingungen („AGB“) gelten für alle Nutzer, Kunden und Unternehmen („Kunde“), welche die unter blackprotect.net bereitgestellte Plattform, APIs, Dashboards, eBPF/XDP-Filterinfrastrukturen oder zugehörige Software („Dienste“) nutzen.

(2) Diese AGB gelten unabhängig davon, ob der Kunde kostenfreie (Beta / Showcase) oder kostenpflichtige Dienstleistungen in Anspruch nimmt.

(3) Abweichende Geschäftsbedingungen des Kunden werden nicht Vertragsbestandteil, es sei denn, BlackProtect hat ihrer Geltung ausdrücklich schriftlich zugestimmt.

(4) Die maßgebliche und rechtlich verbindliche Vertragssprache ist Deutsch. Soweit Übersetzungen (wie Teil II dieser Urkunde) bereitgestellt werden, dienen diese lediglich der Information; bei Widersprüchen geht die deutsche Fassung vor.

(5) Rangfolge: a) Individuelle Sondervereinbarungen in Textform, b) Verbindliche Angebote, c) diese AGB, d) SLA und AUP.

§ 2 Dienstleistungen, Best-Effort-Basis & Formvorschriften

(1) BlackProtect stellt eine Kernel-basierte Netzwerksicherheits- und DDoS-Mitigationsinfrastruktur bereit.

(2) Sämtliche Cybersicherheits- und Schutzdienstleistungen werden auf einer „Best-Effort“-Basis erbracht.

(3) Rechtserhebliche Erklärungen, Nebenabreden oder Garantieversprechen (§ 443 BGB) bedürfen der Schriftform.

§ 3 Konten, Verbot von Mehrfachkonten & Schutzrechte

(1) Max. ein (1) Kundenkonto pro Person/Organisation.

(2) Reverse Engineering, Dekompilierung oder das Ableiten des eBPF/XDP-Bytecodes ist verboten (§ 69e UrhG vorbehalten).

§ 4 Gewerbliche Nutzung, Laufzeiten & Widerruf

(1) Gewerbliche Nutzung setzt kostenpflichtige Tarife voraus. (2) Bei Abonnements gilt grundsätzlich 14 Tage Kündigungsfrist. Verbraucher erhalten den Kündigungsbutton gem. § 312k BGB. (3) Verbrauchern steht ein 14-tägiges Widerrufsrecht zu.

§ 5 Haftung & Haftungsbeschränkungen (§ 521 BGB)

(1) Unentgeltliche Beta-Nutzung: Haftung gemäß § 521 BGB nur für Vorsatz und grobe Fahrlässigkeit. (2) Kostenpflichtige Nutzung: Haftung bei leichter Fahrlässigkeit auf den vorhersehbaren, vertragstypischen Schaden (max. Jahresentgelt) begrenzt.

PART II: TERMS OF SERVICE (ENGLISH TRANSLATION)

Section 1 Scope of Application, Precedence & Legal Language

(1) These Terms of Service ("TOS") apply to all users, customers, and business entities ("Customer") accessing or using the platform, APIs, dashboards, eBPF/XDP filter infrastructures, or associated software ("Services") provided at blackprotect.net.

(2) These TOS apply regardless of whether the Customer uses free services (e.g., Beta, Test, or Showcase access) or paid services. Customer refers to any natural person, legal entity, or partnership with legal capacity.

(3) Conflicting, deviating, or supplementary terms and conditions of the Customer shall not become part of the contract unless BlackProtect explicitly agrees to their validity in text form.

(4) The governing, legally binding language of this agreement is German (Part I). This English translation (Part II) is provided solely for convenience and informational purposes. In the event of any discrepancy or conflict between the German and English versions, the German version shall prevail strictly.

(5) Order of Precedence: In case of conflict, the hierarchy is: a) Individual agreements in text form, b) Binding order confirmations/quotes, c) German TOS (Part I), d) Service Level Agreements (SLA) and Acceptable Use Policy (AUP).

Section 2 Services, Best-Effort Provision & Form Requirements

(1) BlackProtect provides a kernel-based network security and DDoS mitigation infrastructure where management dashboards are decoupled from decentralized edge filter nodes.

(2) All cybersecurity and mitigation services are rendered on a "best-effort" basis. The Customer acknowledges that, according to the current state of technology, absolute protection against cyberattacks, novel attack vectors, or massive volumetric attacks cannot be guaranteed.

(3) Any legally relevant statements, side agreements, commitments, or guarantee promises pursuant to § 443 BGB made on behalf of BlackProtect require written confirmation in text form by the owner or an authorized representative to be legally valid. Informal statements by employees carry no binding effect.

Section 3 Accounts, Prohibition of Multiple Accounts & IP Rights

(1) Each natural person or organization is entitled to maintain a maximum of one (1) user account in the dashboard, unless granted a explicit written exception.

(2) Access credentials, API keys, and authentication tokens must be kept strictly confidential. The Customer is liable for all activities conducted under their account credentials.

(3) Reverse engineering, decompilation, disassembly, or attempting to derive the source code, algorithms, eBPF/XDP bytecodes, or system architecture is strictly prohibited, except as permitted by mandatory statutory law (§ 69e UrhG).

Section 4 Commercial Use, Subscriptions & Termination

(1) Commercial or business-related use of the Services (e.g., protecting monetized games, commercial servers, or ad-supported platforms) requires subscribing to a designated commercial paid plan.

(2) Contract duration and cancellation terms depend on the chosen billing model. Paid subscriptions generally require a 14-day cancellation notice prior to the end of the current billing cycle.

(3) Consumer Rights: Subscriptions with EU consumers (§ 13 BGB) automatically renew indefinitely after the initial period and may be terminated at any time with a maximum notice period of one (1) month (§ 309 No. 9 BGB). BlackProtect provides an easily accessible cancellation button pursuant to § 312k BGB.

Section 5 Liability & Statutory Privilege during Beta Phase (§ 521 BGB)

(1) Gratuitous / Beta Use: To the extent services are provided free of charge during the beta or evaluation phase, BlackProtect's liability is statutory limited under § 521 BGB exclusively to intent and gross negligence. No guarantees or SLAs apply.

(2) Commercial / Paid Use: For paid services, BlackProtect is fully liable for intent, gross negligence, injury to life, body, or health, and mandatory product liability laws. In cases of slight negligence involving essential contractual duties (cardinal obligations), liability is capped at the foreseeable, typical contractual damage, limited to the net amount paid by the Customer in the 12 months preceding the damage event.

Section 6 Acceptable Use Policy (AUP) & Attack Simulator

(1) Authorized Target Protection: The Services may only be used to protect infrastructure owned or legitimately operated by the Customer. The Customer guarantees being the authorized owner or administrator of all registered IP addresses and domains.

(2) Prohibited Activities: It is strictly forbidden to: a) Use the platform to launch, forward, or manage DDoS attacks or malware against third parties; b) Register unauthorized IP targets; c) Attempt to disrupt or overload BlackProtect control panels or filter nodes; d) Use integrated simulation tools (e.g., Attack Simulator) against targets outside authorized test environments.

Section 7 Data Processing & eBPF/XDP Logging

(1) BlackProtect processes technical network data (source/destination IPs, ports, protocol headers, packet rates, and drop reasons such as [XDP_HARDWARE_DROP]) at the kernel level for threat detection.

(2) Legal Basis: Processing is conducted under Art. 6(1)(f) GDPR (legitimate interest in cybersecurity). Technical logs are automatically aggregated and purged.

Section 8 Governing Law & Jurisdiction

(1) This contract is governed exclusively by the laws of the Federal Republic of Germany, excluding the UN Sales Convention (CISG). (2) For B2B customers, exclusive jurisdiction shall be the registered office of the provider.