

Fair Use Policy (FUP)

für IT-, Hosting-, Cloud- und gemeinsam genutzte Dienste

Version	1.0
Stand	04.09.2026
Herausgeber	BORGHESI-DATALINK

Kernaussage

Gemeinsam genutzte Dienste sind für eine faire, sichere und dem gebuchten Produkt entsprechende Nutzung vorgesehen. Dauerhafte Crawler-, Scraper-, Worker-, Massendaten- oder sonstige Spezial-Workloads benötigen eine ausdrücklich dafür geeignete Umgebung und können eine eigene virtuelle oder physische Serverinstanz mit eigener IP-Adresse erfordern.

Diese Fair Use Policy definiert die technischen und betrieblichen Rahmenbedingungen für die Nutzung von Diensten von BORGHESI-DATALINK. Sie soll die Stabilität, Sicherheit, Verfügbarkeit und Reputation gemeinsam genutzter Systeme für alle Kunden schützen.

Soweit diese FUP Bestandteil eines Vertrags, einer Offerte oder der Allgemeinen Geschäftsbedingungen ist, ergänzt sie die dort getroffenen Regelungen. Individuelle schriftliche Vereinbarungen gehen vor.

1. Zweck und Geltungsbereich

Diese Fair Use Policy (FUP) gilt für IT-, Hosting-, Cloud-, Server-, E-Mail-, Storage-, Netzwerk- und vergleichbare Dienste von BORGHESI-DATALINK, soweit diese auf gemeinsam genutzter Infrastruktur bereitgestellt werden oder ausdrücklich auf diese FUP Bezug nehmen.

Sie gilt insbesondere für Shared Webhosting, Managed Hosting, gemeinsam genutzte Web-, Datenbank- und Mailserver, Cloud- und Storage-Dienste sowie weitere Plattformen, bei denen mehrere Kunden dieselben technischen Ressourcen oder öffentlichen IP-Adressen nutzen.

2. Grundsatz der fairen Nutzung

Jeder Kunde darf die bereitgestellten Dienste im Rahmen des gebuchten Produkts und des vertraglich vorgesehenen Nutzungszwecks verwenden. Die Nutzung darf andere Kunden, Systeme oder Dienste nicht unverhältnismässig beeinträchtigen und kein erhöhtes Risiko für Stabilität, Sicherheit oder Reputation der Infrastruktur verursachen.

Die technische Beurteilung erfolgt nicht ausschliesslich anhand einzelner Messwerte. BORGHESI-DATALINK berücksichtigt insbesondere Art, Dauer, Häufigkeit, Parallelität und Auswirkungen einer Nutzung auf CPU, Arbeitsspeicher, Storage-I/O, Datenbanken, Application-Worker, Netzwerk, öffentliche IP-Adressen, Sicherheitsmechanismen und administrativen Betriebsaufwand.

Wichtig

Eine Anwendung kann für einen Shared-Dienst ungeeignet sein, auch wenn zu einem bestimmten Zeitpunkt CPU- oder Speicherauslastung niedrig erscheinen. Dauer, Parallelität, Netzwerkverhalten, externe Sperrrisiken und betriebliche Auswirkungen sind ebenfalls relevant.

3. Vorgesehene Nutzung von Shared-Diensten

Shared-Dienste sind grundsätzlich für typische, dem jeweiligen Produkt entsprechende Anwendungen vorgesehen. Dazu gehören beispielsweise normale Webseiten, CMS-Systeme, Shops, E-Mail-Dienste, Datenbanken und vergleichbare Webanwendungen mit üblichem Ressourcen- und Netzwerkverhalten.

Kurzzeitige Lastspitzen durch legitimes Besucheraufkommen, Updates, Backups oder administrative Arbeiten sind grundsätzlich Teil eines normalen Betriebs, sofern sie nicht dauerhaft oder wiederholt die gemeinsame Infrastruktur beeinträchtigen.

4. Nicht für Shared-Dienste vorgesehene Workloads

Ohne ausdrückliche schriftliche Freigabe sind insbesondere folgende Workloads nicht für Shared-Dienste vorgesehen:

- dauerhafte oder regelmässige Webcrawler, Scraper, Bots und Collector-Prozesse;
- automatisierte Massenerfassung externer Webseiten, APIs, Sitemaps, Feeds oder Datenbestände;
- kontinuierliche Worker-, Queue-, Rendering-, Transcoding-, KI-, Analyse-, Mining- oder vergleichbare Rechenprozesse;
- Anwendungen mit hoher oder dauerhaft erhöhter Parallelität, sehr vielen gleichzeitigen Requests oder kurz getakteten Polling-Intervallen;
- Prozesse, die dauerhaft oder in kurzen Intervallen durch externe Rechner, Browser oder Skripte angestossen werden und serverseitig umfangreiche Verarbeitung auslösen;
- Massendatenverarbeitung, die über den üblichen Betrieb einer Website, eines Shops oder einer Standard-Webanwendung hinausgeht;
- dauerhaft laufende Hintergrundprozesse, eigene Daemons oder Scheduler, sofern diese nicht ausdrücklich Bestandteil des gebuchten Produkts sind;

- Anwendungen, die ungewöhnlich viele ausgehende Netzwerkverbindungen oder grosse Mengen automatisierter Drittanbieter-Abfragen erzeugen.

Solche Anwendungen können eine eigene virtuelle oder physische Serverumgebung, eigene Ressourcen, eigene Sicherheitsregeln und gegebenenfalls eine eigene öffentliche IP-Adresse erfordern.

5. Externe Datenquellen, Crawling und automatisierte Abfragen

Kunden, die automatisiert auf externe Dienste, Webseiten, APIs oder andere Datenquellen zugreifen, sind selbst dafür verantwortlich, dass diese Zugriffe rechtmässig, technisch angemessen und mit den Bedingungen der jeweiligen Drittanbieter vereinbar sind.

- Rate Limits, robots.txt, API-Vorgaben, Nutzungsbedingungen und sonstige technische Begrenzungen externer Anbieter sind zu beachten, soweit sie anwendbar sind.
- Automatisierte Zugriffe dürfen nicht so betrieben werden, dass gemeinsame Server-IP-Adressen wegen Bot-, Abuse- oder Scraping-Verhaltens gesperrt, gedrosselt oder negativ bewertet werden können.
- Drittanbieter-Abfragen mit erheblicher Parallelität oder dauerhaftem Volumen gehören grundsätzlich in eine dafür geeignete, isolierte Umgebung.

6. Schutz der gemeinsamen IP-Reputation

Öffentliche IP-Adressen von Shared-Systemen sind Teil der gemeinsam genutzten Infrastruktur. Eine negative Reputation oder Sperre kann mehrere Kunden gleichzeitig betreffen.

Kunden dürfen deshalb keine Anwendungen betreiben, deren Verhalten mit erhöhter Wahrscheinlichkeit dazu führt, dass gemeinsame IP-Adressen bei externen Plattformen, Spamfiltern, Abuse-Systemen, Firewalls, Rate-Limit-Systemen oder Reputation-Diensten gesperrt, gedrosselt oder negativ bewertet werden.

BORGHESI-DATALINK kann verlangen, dass eine solche Anwendung auf eine eigene Umgebung mit eigener öffentlicher IP-Adresse migriert wird.

7. Sicherheitsmechanismen und Whitelisting

Firewall-, Fail2Ban-, IDS/IPS-, WAF-, Rate-Limit-, Anti-Spam- und vergleichbare Schutzmechanismen dienen dem Schutz der gesamten Infrastruktur. Sie dürfen nicht umgangen, manipuliert oder eigenmächtig deaktiviert werden.

Ein Kunde hat keinen Anspruch darauf, dass Schutzmechanismen dauerhaft deaktiviert, abgeschwächt oder durch umfassende Sonderfreigaben umgangen werden, um eine für den gebuchten Shared-Dienst ungeeignete Anwendung zu ermöglichen.

Wenn eine legitime Anwendung wiederholt Sicherheitsmechanismen auslöst, kann BORGHESI-DATALINK statt weiterer Ausnahmen die Migration auf eine eigene Serverumgebung verlangen. Eine zeitweise oder individuelle Whitelist stellt keine Zusicherung dar, dass diese dauerhaft bestehen bleibt.

8. Auswirkungen auf andere Kunden und Dienste

Kein Kunde darf einen Dienst so verwenden, dass dadurch andere Kunden, Dienste oder interne Betriebsprozesse beeinträchtigt werden können. Dabei muss eine konkrete Störung nicht bereits eingetreten sein. Ein nachvollziehbares erhöhtes Risiko für Stabilität, Sicherheit, Verfügbarkeit oder IP-Reputation kann ausreichen, um technische Massnahmen oder eine Migration zu verlangen.

BORGHESI-DATALINK muss nicht abwarten, bis andere Kunden tatsächlich ausfallen oder eine gemeinsame IP-Adresse bereits extern gesperrt wurde.

9. Weitere unzulässige oder genehmigungspflichtige Nutzung

Unabhängig von der Ressourcenfrage sind insbesondere folgende Nutzungen unzulässig oder nur nach ausdrücklicher Vereinbarung zulässig:

- Versand von Spam, unerwünschter Massenwerbung oder missbräuchlichen automatisierten Nachrichten;
- Betrieb oder Verteilung von Schadsoftware, Phishing, Credential-Harvesting oder anderen sicherheitsgefährdenden Inhalten;
- Angriffe, Portscans, Brute-Force-Aktivitäten oder der Betrieb von Infrastruktur zur Umgehung von Sicherheitsmassnahmen;
- Krypto-Mining oder vergleichbare dauerhaft rechenintensive Spezial-Workloads auf Shared-Systemen;
- Nutzung, die gegen geltendes Recht, Rechte Dritter oder verbindliche vertragliche Vorgaben verstösst.

10. Technische Massnahmen bei übermässiger oder ungeeigneter Nutzung

Stellt BORGHESI-DATALINK fest, dass eine Nutzung dem gebuchten Produkt nicht entspricht oder ein relevantes Betriebsrisiko darstellt, können angemessene technische Massnahmen getroffen werden. Dazu gehören insbesondere:

- Kontaktaufnahme mit dem Kunden und Aufforderung zur Anpassung der Anwendung;
- Rate Limits, Ressourcenbegrenzungen oder Einschränkung einzelner Funktionen;
- vorübergehende Deaktivierung einzelner Prozesse oder Dienste;
- Sperrung sicherheitskritischer Zugriffe oder Endpunkte;
- Aufforderung zur Migration auf eine geeignete eigene VM oder einen dedizierten Server.

Bei unmittelbarer Gefährdung von Sicherheit, Stabilität oder anderen Kunden kann BORGHESI-DATALINK erforderliche Schutzmassnahmen ohne vorherige Ankündigung treffen. Der Kunde wird anschliessend so bald wie praktisch möglich informiert.

11. Migration auf eigene Infrastruktur

Ist eine Anwendung hinsichtlich Lastprofil, Dauerbetrieb, Parallelität, Sicherheitsanforderungen oder externer Netzwerkaktivität nicht für Shared Hosting geeignet, kann BORGHESI-DATALINK die Verlagerung auf eine eigene technische Umgebung verlangen.

Je nach Anwendung kann dies insbesondere eine eigene virtuelle Maschine, einen dedizierten Server, eigene Ressourcenlimits, eine eigene Datenbank, eigene Worker und eine eigene öffentliche IP-Adresse umfassen.

Grundsatz

Dass eine Anwendung zuvor auf einem Shared-System betrieben werden konnte, begründet keinen Anspruch darauf, diese Betriebsform dauerhaft fortzuführen. Entscheidend ist die aktuelle technische Nutzung und deren Eignung für das gebuchte Produkt.

12. Administrativer Mehraufwand

Aussergewöhnlicher Administrations- und Analyseaufwand, der durch eine nicht vertragsgemässe oder für das gebuchte Produkt ungeeignete Nutzung entsteht, kann nach dem jeweils gültigen Support- oder Dienstleistungstarif verrechnet werden, sofern dieser Aufwand nicht Bestandteil des gebuchten Produkts ist.

Dies kann beispielsweise die wiederholte Analyse von Sperren, Abuse-Ereignissen, Firewall- oder Fail2Ban-Ausnahmen, Ressourcenproblemen, IP-Reputation, ungewöhnlichem Netzwerkverkehr oder durch kundenseitige Anwendungen ausgelösten Störungen umfassen.

13. Ausnahmen und individuelle Vereinbarungen

Für besondere Anwendungen können individuelle technische und vertragliche Vereinbarungen getroffen werden. Eine Ausnahme gilt nur im ausdrücklich vereinbarten Umfang und kann an Ressourcenlimits, Sicherheitsvorgaben, Zusatzkosten oder eine separate Infrastruktur gebunden sein.

Ein vorübergehend geduldeter Zustand oder eine einmalige technische Sonderfreigabe stellt keine dauerhafte Änderung des vereinbarten Leistungsumfangs dar.

14. Versionierung und Aktualisierung

BORGHESI-DATALINK überprüft diese FUP regelmässig und kann sie an technische Entwicklungen, Sicherheitsanforderungen, Produktänderungen und betriebliche Erfahrungen anpassen. Jede veröffentlichte Fassung erhält eine Versionsnummer und ein Datum.

Für neue Verträge oder neu einbezogene Leistungen kann die jeweils aktuelle Fassung verwendet werden. Für bestehende Vertragsverhältnisse richtet sich die Wirksamkeit einer geänderten Fassung nach den vereinbarten Vertrags- und AGB-Regelungen. Eine neue FUP-Version ersetzt nicht automatisch abweichende individuelle Vereinbarungen.

Versionshistorie

Version	Datum	Status	Änderung
1.0	04.09.2026	Erstfassung	Einführung einer allgemeinen FUP für gemeinsam genutzte IT-, Hosting- und Cloud-Dienste.

15. Vorrang individueller Vereinbarungen und Schlussbestimmung

Individuelle schriftliche Vereinbarungen, Leistungsbeschreibungen oder speziell zugesicherte Ressourcen gehen dieser FUP vor. Im Übrigen ergänzt die FUP die jeweiligen Vertragsunterlagen, soweit sie wirksam einbezogen wurde.

Diese FUP beschreibt technische und betriebliche Nutzungsgrundsätze. Sie ersetzt keine individuelle rechtliche Beratung und keine gesetzlich zwingenden Regelungen.

BORGHESI-DATALINK

Fair Use Policy v1.0 | Stand 04.09.2026