

bright data

Ethics & Compliance Non-Negotiables

How the web data infrastructure industry defines responsible infrastructure and the benchmark for consented, transparent, and independently validated operations

Ethics & Compliance Top Priorities

Practitioners are clear about what they need. These are the essentials, ranked by the industry itself.



Transparency & traceability of data sources

64%



Clear legal review & documented compliance

52%



Ability to access data at scale without being blocked

51%



Minimizing disruption (rate limiting, respectful access)

45%



Avoiding collection of sensitive or personal data

40%



Fair access for smaller organizations

38%

The Risks Are Real and Practitioners Know It

These are the top compliance and ethical failure modes businesses face in real world data collection scenarios. Most businesses report these face several of these obstacles at once, but relying on a consented network provides a viable solution.



Collecting sensitive / identifiable data

45%



Non-compliance with laws /standards

41%



Lack of transparency or consent

40%



Accessing data behind paywalls / logins

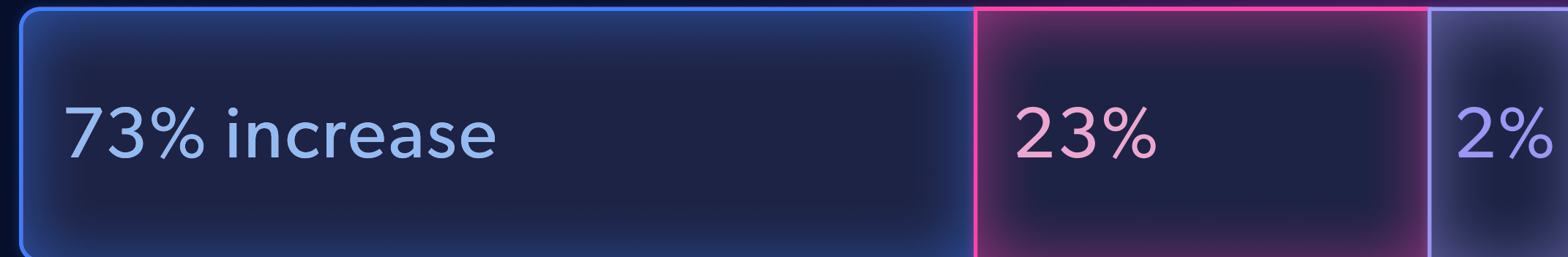
37%

More Challenges Ahead

88% of respondents agree that access to public web data is becoming increasingly restricted. The compliance paradox is real and growing.

Businesses are concerned challenges will increase

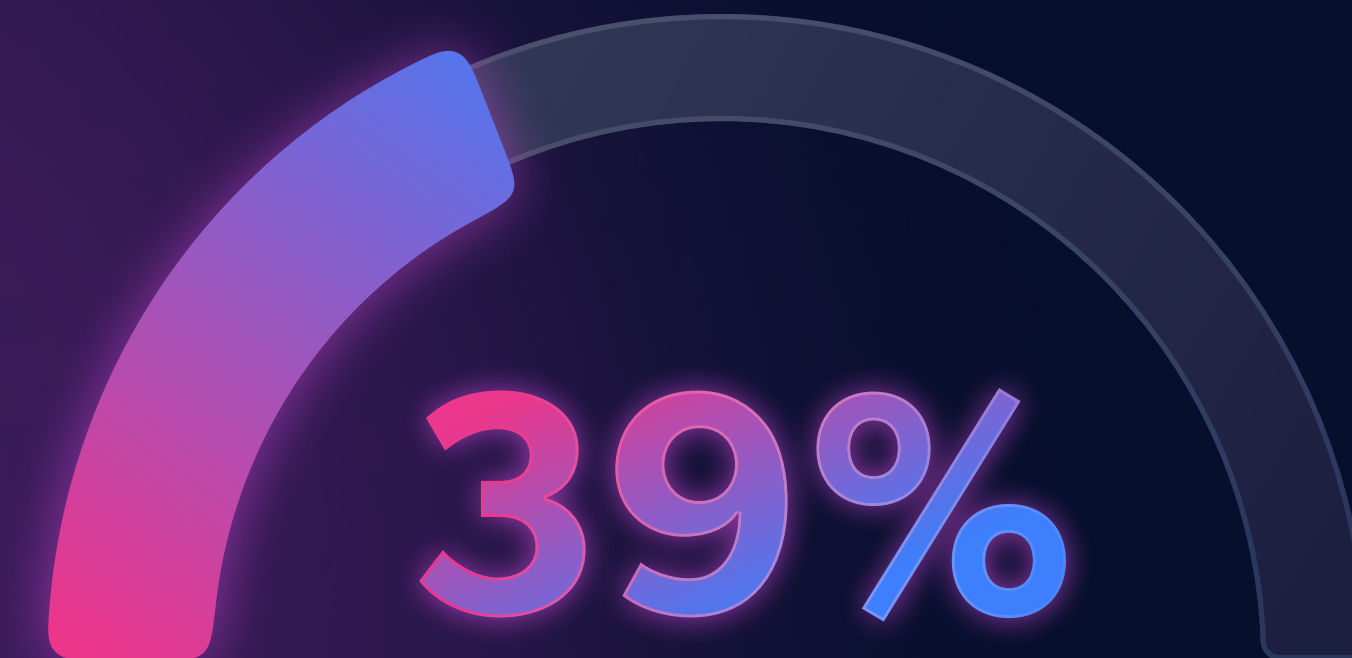
Regulatory Legislation



Website blocking



Creates greatest friction



of businesses say regulatory restrictions **create the greatest friction**. A vendor must be able to navigate these with **ease and provide proof of their compliance**.



AI demands **more web data** while regulation and blocking simultaneously **increase**. Organizations built on opaque or unconsented infrastructure face mounting legal and reputational risk.

Two Types of Networks. One Clear Choice.

Not all proxy networks are created equal. The distinction between unconsented and consented infrastructure is fundamental.

Unconsented / Malicious

- ✗ Built from **stolen infrastructure**, devices recruited without user knowledge.
- ✗ Internet connection sold to **anonymous buyers** for **anonymous purposes**.
- ✗ **No KYC**, no governance, no accountability, no opt-out.
- ✗ Recruited through **undetectable means**, often used for nefarious purposes.

Consented / Responsible

Enforces four distinct tiers of transparency:

- ✓ **Sourcing:** Every IP comes from a peer who knowingly consented via a standalone screen and can opt out at any time.
- ✓ **Vetting:** Documented KYC vets every customer. Partners are reviewed before joining the program.
- ✓ **Governance:** Abuse is detected, blocked, and attributed in real time. Researcher reports are acted on fast.
- ✓ **Accountability:** Independent audits. Outside researchers probe the network for criminal-pool overlap.

Setting a New Industry Standard

Bright Data's opt-in process is the most rigorous user consent framework in the industry, every element is explicit, proactive, and documented.

1

Standalone dedicated opt-in screen
never buried in legal text or a T&S scroll.

2

Six explicit disclosures
intended use, access limits, who Bright Data is, opt-out path, Privacy Policy link, EULA link.

3

Users can opt-out at any time
in two steps directly from app settings, no hoops, no friction.

4

Concrete value exchange:
ad-free experience, premium features, or in-app rewards. Users can still use the app if they decline.

5

Whitelist-only domain access
malicious, private, or unauthorized sites cannot be accessed through a peer's device.

6

Every app partner is reviewed
by Bright Data's compliance team before joining the SDK program. Not all applicants are approved.

Privacy by Architecture, Not by Promise

Technical safeguards are embedded into every layer of the network, not bolted on as an afterthought.



Peer-Server-Peer

All data passes through Bright Data's servers. No peer ever contacts another peer directly.



No Personal Data

No cookies, no device IDs, no browsing history, no PII — ever. Only the IP is temporarily and anonymously used.



Minimal Bandwidth

~50MB/day on Wi-Fi (≈30 sec of Netflix 4K). ~5MB/day on cellular (≈1 Spotify song).



Device-Aware

Only runs when device is idle, plugged in or charged, and on Wi-Fi. If device is busy, processes sleep immediately.



Whitelist Only

Only pre-approved domains accessible. IPv4/IPv6 blacklists enforced at backend and SDK layer independently.



HTTP/HTTPS Only

All other ports blocked. Rate limits enforced. Local and private networks fully protected via multi-layer safeguards.

bright data

Bright Data is the Benchmark for Responsible Infrastructure

Trust Center

brightdata.com/trustcenter

AppEsteem Certification

customer.appesteem.com/certified

PwC Report

brightdata.com/trustcenter/pwc-report

Privacy Policy

brightdata.com/privacy

Alliance for Responsible Data

responsibledatacollection.org

ISO 27001 / 27017 / 27018 & SOC 2 Type II

"Security, transparency, and responsibility are baseline requirements at Bright Data."

Or Lenchner, CEO, Bright Data