

key findings missing

Key Takeaways:

key takeaways missing

Key Recommendations:

key recommendations missing

Services evaluated:



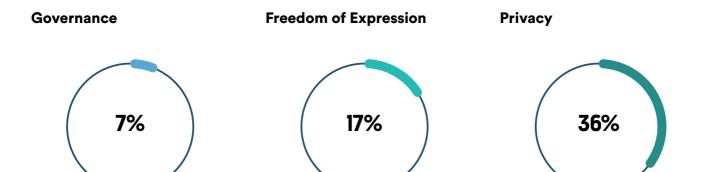
Taobao.com



AliGenie

The 2020 RDR Index covers policies that were active between February 8, 2019 and September 15, 2020. Policies that came into effect after September 15, 2020 were not evaluated for this Index.

Scores reflect the average score across the services we evaluated, with each service weighted equally.



We rank companies on their approach to governance, and their policies and practices that affect freedom of expression and privacy.

Governance 7%

governance missing

Indicators		
G1. Policy Commitment		0%
G2. Governance and management oversight		0 70
		8%
G3. Internal implementation	1	19%
G4. Human rights due diligence	~	0%
G5. Stakeholder engagement and accountability		0%
G6. Remedy and appeals	~	
		15%

Freedom of Expression 17%

freedom of expression missing

Indicators	
F1. Access to policies	∨ 51%
F2. Notification of policy changes	> 9%
F3. Process for policy enforcement	× 42%
F4. Data about policy enforcement	~
F5. Process for responding to third-party requests to restrict content or accounts	0% V 11%
F6. Data about government demands to restrict for content and accounts	0%
F7. Data about private requests for content or account restriction	0%
F8. User notification about content and account restriction	19%
F9. Network management (telecommunications companies)	NA
F10. Network shutdown (telecommunications companies)	NA
F11. Identity policy	0%
F12. Algorithmic content curation, recommendation, and/or ranking systems	
F13. Automated software agents ("bots")	35%
	NA

Privacy 36%

privacy missing

Indicators		
P1. Access to policies affecting users' privacy	~	38%
P2. Notification of changes	~	18%
P3. User information collection and inference	~	
P4. Sharing of user information		50%
P5. Purpose for collecting, inferring, and sharing user information		52%
P6. Retention of user information		60%
P7. Users' control over their own user information		17%
P8. Users' access to their own user information		35%
P9. Collection of user information from third parties		8%
P10. Process for responding to demands for user information	~	2%
P11. Data about demands for user information	~	0%
P12. User notification about third-party requests for user information		33%
P13. Security oversight		
P14. Addressing security vulnerabilities		67%
P15. Data breaches		36%
		83%

P16. Encryption of user communication and private content (digital platforms)	38%
P17. Account security (digital platforms)	58%
P18. Inform and educate users about potential risks	50%