

key findings missing

Key Takeaways:

key takeaways missing

Key Recommendations:

key recommendations missing

Services evaluated:



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.

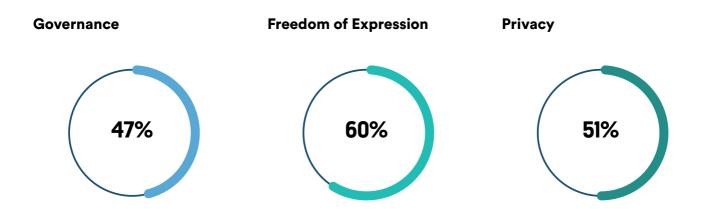
Scores reflect the average score across the services we evaluated, with each service weighted equally.

Changes since 2019:



analysis missing

Gained 0.27 points on comparable indicators since the 2019 RDR Index.



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

Governance 47%

governance missing

Indicators

G1. Policy Commitment		67%
G2. Governance and management oversight		
		75%
G3. Internal implementation		
		63%
G4. Human rights due diligence	~	
		2%
G5. Stakeholder engagement and accountability		
		50%
G6. Remedy and appeals	~	060/

Freedom of Expression 60%

freedom of expression missing

Indicators

F1. Access to policies	71%
F2. Notification of policy changes	V 16%
F3. Process for policy enforcement	V 68%
F4. Data about policy enforcement	× 37%
F5. Process for responding to third-party requests to restrict content or accounts	× 85%
F6. Data about government demands to restrict for content and accounts	80%
F7. Data about private requests for content or account restriction	60%
F8. User notification about content and account restriction	63%
F9. Network management (telecommunications companies)	NA NA
F10. Network shutdown (telecommunications companies)	NA NA
F11. Identity policy	100%
F12. Algorithmic content curation, recommendation, and/or ranking systems	30%
F13. Automated software agents ("bots")	
	50%

Privacy 51%

privacy missing

Indicators

P1. Access to policies affecting users' privacy	~	50%
P2. Notification of changes	~	
P3. User information collection and inference	~	25%
P4. Sharing of user information		50%
P5. Purpose for collecting, inferring, and sharing user information		63%
P6. Retention of user information		60%
To Recention of user information		40%
P7. Users' control over their own user information		25%
P8. Users' access to their own user information		750/
P9. Collection of user information from third parties		75%
P10. Process for responding to demands for user information	~	33%
P11. Data about demands for user information	~	50%
P12. User notification about third-party requests for user information		43%
P13. Security oversight		67%
P14. Addressing security vulnerabilities		67%
THE Floring scounty value abilities		50%
P15. Data breaches		0%

P16. Encryption of user communication and private content (digital platforms)	
	25%
P17. Account security (digital platforms)	1000/
	100%
P18. Inform and educate users about potential risks	100%
	10070