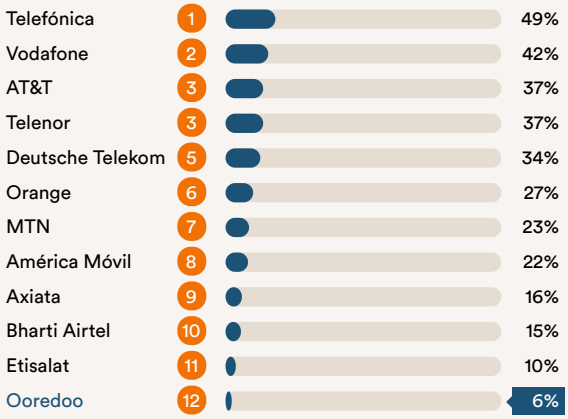
Telecommunications companies

Ooredoo Q.P.S.C.

Rank: 12th **Score:** 6%

Headquartered in Qatar, Ooredoo provides telecommunications services such as mobile, broadband, and fiber in 13 countries in the Middle East, North Africa, and south and southeast Asia. In the fourth quarter of 2019, it had 117 million users.



- **For the first time since it was added to the RDR Index in 2017, Ooredoo disclosed a privacy policy.** However, the company continued to lack transparency about its handling of user information and continued to lag behind on policies affecting freedom of expression. Throughout 2019 and 2020, Ooredoo's subsidiaries imposed network shutdowns at the behest of several governments, notably suspending mobile internet services in Rakhine and Chin states in Myanmar amid clashes between government troops and ethnic insurgents. Ooredoo also restricted access to its networks in Algeria and Iraq during anti-government protests, and its local subsidiary continued to block access to VoIP apps, which are banned in Qatar. The company offered minimal transparency about how it handles government demands to restrict services.

Key Takeaways

- Ooredoo received the lowest score of all telecommunications companies, and was slightly outperformed by Etisalat, the other Middle Eastern company ranked in the RDR Index.
- Ooredoo did not commit to respect users' freedom of expression or privacy in accordance with international human rights standards.
- Despite finally making its privacy policy available to the public, Ooredoo lacked transparency about its handling of user information.

Key recommendations

- Commit to human rights. Ooredoo should commit to respecting users' rights to privacy and freedom of expression in accordance with international human rights standards.
- Be transparent about government censorship demands. Ooredoo should publish policies clearly outlining its processes for responding to government demands to block websites and restrict access to networks and services.
- Be transparent about handling user information. Ooredoo should describe which types of user information it shares and with whom, and how long it retains this information.

Services evaluated:

Prepaid mobile

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

Postpaid mobile

Fixed-line broadband

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

Lead researchers: Afef Abrougui, Zak Rogoff

Operating company evaluated:
Ooredoo Qatar

For telecommunications companies, the RDR Index evaluates relevant policies of the parent company, the operating company, and selected services of that operating company.

Market cap: $6.58 billion (As of Feburary 4, 2021)

QSE: ORDS

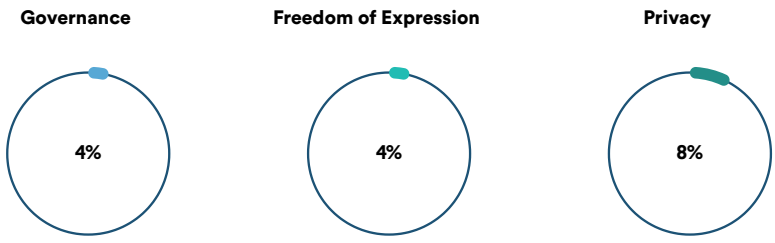
Website: https://www.ooredoo.qa

Changes since 2019

- Ooredoo disclosed more about its governance by providing new information about how it trains its employees on privacy, though it did not show how comprehensive or regular these trainings are.
- Ooredoo increased its transparency about how it manages user information by describing what type of information it collects and its purposes for doing so.
- Ooredoo improved its security measures to protect user data, making a commitment to notify authorities of data breaches when they occur, though the commitment is vague.

+ 5.63 points

Gained 5.63 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 4%

Eastern company in the RDR Index.

- **Commitment to human rights:** In its Customer Charter, Ooredoo committed to respecting privacy as a "legal right" in Qatar, falling short of committing to respecting this privacy in accordance with international human rights standards. It did not commit to respecting human rights in its use and development of algorithmic systems (G1).
- **Human rights due diligence:** Ooredoo did not publish any evidence that it conducted due diligence to assess human rights impacts or risks associated with its operations, products, or services (G4).
- **Stakeholder engagement:** Ooredoo continued to disclose no systematic engagement with stakeholders that represent, advocate on behalf of, or are people whose privacy and freedom of expression and information are directly impacted by the company (G5).
- **Remedy:** Ooredoo did not provide users with grievance or remedy mechanisms to address their privacy and freedom of expression and information complaints (G6a). The mechanism offered in its Customer Charter is only named "unethical sales or customer service behavior," offering no evidence that users can file grievances based on potential violations of their rights.

Freedom of Expression 4%

Ooredoo was not transparent about its policies affecting users' freedom of expression and information, revealing only scant information about its enforcement processes and policies on network shutdowns.

- **Content moderation:** While Ooredoo 's terms and conditions outlined the types of content and activities it does not permit on its services and why it may restrict users' accounts, the company was silent on how it enforces these and other rules (F3a). It did not disclose any data about content and account restrictions to enforce its terms of service (F4a, F4b) and did not commit to notifying users of such restrictions (F8).
- **Advertising content and targeting:** Despite providing a SMS service that enabled businesses to target users with ads, Ooredoo did not provide policies outlining its ad content and ad targeting practices (F1b, F1c, F3b, F3c). It did not publish data on ads removed to enforce these rules (F4c).
- **Network management:** Ooredoo did not commit to respecting network neutrality (F9). While it provided vague reasons for why it may shut down service to a particular area or group of users—for instance, "if any competent authority prohibits the provision of the Service in Qatar"—it did not disclose any other policy information elucidating how it would respond to a government shutdown demand (F10). It did not explain why it may restrict access to specific apps and protocols, including VoIP apps (which are outlawed in Qatar), nor did it commit to push back against these types of demands.
- **Censorship demands:** Ooredoo did not disclose a policy for handling third-party demands to remove content and accounts, including government demands (F5-F7). Article 21 of Qatar's Cybercrime Prevention Law imposes a variety of obligations on operators, including requiring them to block access to content at the request of judicial authorities. However, there are no regulations in Qatar that prohibit companies from disclosing their process for handling government or private demands to restrict access to content or accounts or publishing data about these demands.

Privacy 8%

Ooredoo revealed the least out of the 12 ranked telecommunications companies about its policies affecting users' privacy, though it showed the first signs of progress by publishing a privacy policy.

- **Handling of user data:** For the first time since we added it to the RDR Index in 2017, Ooredoo published a privacy policy. While the policy was easy to find and understandable, it was not available in Arabic, one of

user information with legal authorities, the company revealed nothing about its data sharing policies, including which user information it shares, with whom, and for what purposes (P4, P5). It was also silent about its data inference policies (P3b), how long it retains user information (P6), and options for users to control and access their information (P7, P8).

- **Government and private demands for user data:** Ooredoo did not disclose a policy for handling third-party demands for user information, including government demands (P10-P12). There are no regulations in Qatar that prohibit companies from disclosing their process for handling such demands.
- **Security:** Apart from a vague commitment to notify authorities of data breaches that "may cause serious damage" (P15), Ooredoo did not publish any security policies. For example, it did not publicly describe any internal processes to keep user information secure, such as systems to limit and monitor employee access to user information or an audit mechanism overseen by an internal security team (P13). It also did not provide a bug bounty program, a practice through which many companies enable technical researchers to submit reports of security vulnerabilities (P14).