Cyber Security at Duolingo

Protecting the privacy and security of our customers' personal and financial data is important to Duolingo. We protect our customers' privacy by minimizing collection of sensitive data and being transparent about our data collection and usage, as detailed in our privacy policy.

Our data security processes are also structured and comprehensive. At the employee level, we conduct regular phishing exercises and maintain strict firewalls to detect exploitation attempts and mitigate DDoS attacks. We also provide employee training on data privacy and cybersecurity best practices, both annually and as part of onboarding. To mitigate risk and identify potential vulnerabilities, we review our security practices quarterly and conduct penetration testing and cloud security assessments.

We have also maintained General Data Protection Regulation ("GDPR") compliance since 2018 and have received our SOC 2 Type I attestation, which is audited annually by a third party for recertification. In addition, we conduct quarterly reviews of our cyber program.

In 2024, we are looking towards ISO 27001 certification for the Duolingo English Test, which requires more sensitive data than the Duolingo learning app. As we work to strengthen our security processes, we understand that risks can come from our partners. We assess the cyber security program of every new relevant third-party contract or renewal contract and privilege those with cyber security certification. In case a partner does not have a certification that meets our standards, we have a vetting process in place to ensure alignment with our standards.

In the unlikely event of a breach, we maintain a response playbook to promptly investigate, contain, and remediate any potential impact on our customers. Throughout the year, we test our cyber security response playbook with regular tabletop exercises, which include both leadership from different departments and engineers focusing on incident response readiness.

While we recognize that no system is foolproof, to date we have not had any material data breaches, loss of data or successful cyber-attacks. The Audit Committee of the Board oversees the Company's cyber security processes and is brief on it at least annually.