Mail.Ru Group considers security and user data protection to be one of its top priorities.

All of our products are offered with the most effective security systems designed to protect user data. This includes our email, social media, games, messengers, e-commerce, and all other Mail.Ru Group services.

We use data encryption

To ensure the security of user email and content downloaded on social media or messengers, we encrypt data using a multi-level security system built on advanced technologies such as DKIM, DMARC, TLS, HTTPS, HSTS, HTTPonly cookie, Secure Cookie and Content Security Policy.

We also offer two-factor authentication for the Mail.Ru Email and Cloud services and also on the social networks. TLS is implemented in A+ rating configuration (according to Qualys SSL Labs) with PFS and HSTS supported for all compatible clients.

For the VKontakte social network, we use HTTPS, HSTS, Certificate Pinning, Secure Cookie, CORS and Content Security Policy.

Indentification of potential threats

We operate a constant monitoring system for the security of our services as well as the infrastructure they are based upon. We also guarantee protection against spam, malware, viruses and other threats. In April 2014, we launched a program for the identification of vulnerabilities in our Email service and Mail.Ru Portal projects implemented on the HackerOne global platform.

We have respond to government requests for specified data of selected users in accordance with applicable laws of appropriate jurisdictions. These requests are thoughly reviewed by our legal team. We reject requests that appear to be insufficient or too vague. All of our interaction with state authorities is based exclusively on principles set out in the relevant legislation of the jurisdiction where our users are held liable.

Our social networks give users the option to customize the privacy of their data. Our services also allow users to choose the information they are willing to share.

Mail.Ru Group remains politically neutral. At no time do we support, directly or indirectly, any political party or ideology. In the event that we believe certain legislative initiatives should be reconsidered, we are dedicated to providing an evaluation of the issue to the authorities based upon our expertise.

Internal control

Our Audit Committee has the primary function of supporting the Board of Directors in its duties pertaining to supervising the effectiveness of the Group's internal control system, including that of internal audit and risk management functions.

Internal control is exercised by the Board of Directors, executive bodies, officers and other Company employees to make sure Mail.Ru Group meets its targets in the following areas:

- Business activity efficiency and effectiveness within the Company
- Reliability and credibility of the Company's reporting
- Compliance with the requirements of regulatory acts and internal documents of the Company.

The Internal Audit Department carries out internal audits, reviews and other engagements with respect to Mail.Ru Group subsidiaries, assesses the effectiveness of the internal control system of Mail.Ru Group including its subsidiaries and associates, and issues recommendations following these assessments.

Mail.Ru Group is subject to certain risks that affect our ability to operate, serve our clients, and protect our assets. Controlling these risks through a formal program is necessary for the Group's well-being. Our Board of Directors is also responsible for the comprehensive governance of risks, overseeing overall adequacy and effectiveness of risk management. Mail.Ru Group is

committed to identifying and managing risks in line with the best international corporate governance practices.