# DATA POLICY

Mail.Ru Group considers security and user data protection to be its top priority.

All of our products develop and constantly update 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.

## Data encryption

To ensure the security of user data, our products encrypt and protect 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 as well as on VK and OK.
TLS is implemented in A+ rating configuration (in accordance with Qualys SSL Labs standard) with PFS and HSTS supported for all compatible clients. For the VK and OK, we use HTTPS, Secure Cookie, CORS and Content Security Policy. VK also uses HSTS and Certificate Pinning.

## Preventing potential threats

We operate a constant monitoring system for the security of our services as well as the infrastructure they are based upon. We work hard to protect against spam, malware, viruses and other threats. In addition to that, in order to constantly test the effectiveness of our systems. In April 2014, we launched a program to identify vulnerabilities on the HackerOne global platform.

Our social networks give users the option to customize the privacy of their 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.

## Preventing spread of inappropriate information

Any VK and OK user can report content they deem to be inappropriate or offensive with the ‘Report’ button. We consider complaints and react in the shortest time possible: content in violation of the law or rules of the website is deleted, and offenders are blocked. Response time is normally just a few minutes and is never more than one hour.

## Respond to government requests

We respond to requests from government agencies in various countries where we operate for specified data of selected users in accordance with applicable laws. These requests are thoroughly reviewed by our legal teams. We reject requests that do not comply with the applicable legislation.

## Legislation

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 in data protection.

The Internal Audit Department performs IT audits which include assessments of the security and effectiveness of the Group’s information systems in relation to the confidentiality, integrity, and availability of data as well as data processing.

We have a designated Data Protection Officer who ensures that of our products comply with data protection principles. We also periodically and systematically arrange training programs for our employees related to data processing and security.

**Mail.Ru Group complies with the applicable data protection laws, including GDPR**

We are committed to comply with the applicable data protection laws.

As part of our GDPR preparation process, we have revised and updated all our internal processes and procedures including data systems, implementation of the Data Impact Assessment and documentation in order to ensure full compliance with the GDPR.

We use technical and organizational measures to ensure data security by default. We have revised our privacy and Cookies policies for our end users as well as the wording of our consent forms and independent processes used to obtain direct marketing consent, including clear opt-in mechanisms for marketing subscriptions. We use a clear and transparent notification system with the option to unsubscribe from any of our marketing materials.

We always conduct Data Protection Impact Assessments whenever processing is large in scale, can result in a high risk to the rights and freedoms of individuals, or includes special category/criminal conviction data. In order to carry out impact assessments that comply fully with the GDPR requirements, we have developed special assessment procedures that allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

We neither obtain nor process any special categories data purposefully. We notify our users in our Privacy Policies that they should avoid sharing this kind of information through our products and services.

We provide easy access to our support services. Our support agents are always happy to help our users exercise their individual rights. We respond to and fulfill requests from data owners with respect to their rights to data portability, access, rectification, and erasure. We also help exercise other data owner rights specified in the GDPR (e.g. right to

object to processing for the purposes of direct marketing where such direct marketing exists).