Утверждено советом директоров Mail.Ru Group Limited

ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ДАННЫХ

Безопасность и защита пользовательских данных – главный приоритет в работе компании Mail.Ru Group.

Мы разрабатываем и постоянно обновляем надежные системы защиты пользовательских данных для всех наших продуктов, включая электронную почту, социальные сети, игры, мессенджеры, e-commerce и другие сервисы Mail.Ru Group.

Шифрование данных

Для обеспечения безопасности пользовательских данных, в продуктах компании применяются многоуровневые системы шифрования и защиты целостности данных, основанные на таких передовых технологиях, как DKIM, DMARC, TLS, HTTPS, HSTS, HTTPonly cookie, Secure Cookie и Content Security Policy.

Также мы предлагаем двухфакторную аутентификацию пользователей для сервисов электронной почты и облачного хранения данных Mail.Ru, а также в социальных сетях ВКонтакте и Одноклассники.
Протокол TLS используется в конфигурации уровня A+ (в соответствии со стандартами Qualys SSL Labs) с применением механизмов PFS и HSTS при условии их поддержки со стороны пользователя. В социальных сетях ВКонтакте и Одноклассники мы используем протоколы HTTPS, Secure Cookie, CORS и Content Security Policy. ВКонтакте также использует HSTS и Certificate Pinning.

Предотвращение потенциальных угроз

Наша система мониторинга работает в постоянном режиме для обеспечения безопасности наших услуг и сопутствующей инфраструктуры. Мы усердно боремся со спамом, вредоносными программами, вирусами и другими угрозами. Кроме того, в апреле 2014 года мы запустили программу по выявлению уязвимостей на базе глобальной платформе HackerOne для перманентной проверки эффективности наших систем.

Пользователи наших социальных сетей имеют возможность настроить приватность своих данных по своему усмотрению. При пользовании нашими услугами потребители выбирают, какими данными они готовы делиться.

Предотвращение распространения ненадлежащей информации

Любой пользователь социальных сетей ВКонтакте и Одноклассники может сообщить о неправомерном или оскорбительном, по его мнению, контенте с помощью кнопки «Пожаловаться». Мы рассматриваем жалобы пользователей и реагируем максимально оперативно — материалы, которые нарушают правила сайта или законодательство, удаляются, а нарушители — блокируются. Время реакции не превышает одного часа, а обычно составляет несколько минут.

Запросы от государственных органов

Запросы на получение данных конкретных пользователей со стороны государственных органов разных стран, где мы работаем, мы рассматриваем в соответствии с применимым законодательством. Наши юристы тщательно изучают все поступающие запросы. Мы отвечаем отказом на запросы, не соответствующие требованиям применимого законодательства.

Законодательство

Mail.Ru Group придерживается принципа политического нейтралитета. Компания никаким образом не выражает прямой или косвенной поддержки какой-либо политической партии или идеологии. В случае если мы видим, что некоторые законодательные инициативы нуждаются в доработке или пересмотре, мы считаем своим долгом предоставить свою экспертную оценку по данному вопросу ответственным органам.

Внутренний контроль

Задача нашего аудиторского комитета – поддерживать функцию совета директоров по надзору за эффективностью работы системы внутреннего контроля, включая внутренний аудит и оценку рисков в безопасности данных.

Внутренний аудиторский департамент проводит аудиты IT-систем, включающие оценку безопасности и эффективности информационных систем Компании с точки зрения конфиденциальности, целостности и доступности данных и их обработки.

Сотрудник по защите данных обеспечивает соответствие наших продуктов стандартам безопасности данных. Также мы периодически и систематически проводим тренинг-программы для наших сотрудников по вопросам безопасности и обработки данных.

Mail.Ru Group действует в рамках законов по защите данных, включая GDPR

Мы придерживаемся принципов соблюдения применимых законов о персональных данных.

В рамках подготовки к применению Общего регламента по защите данных (GDPR), мы обновили и проверили все внутренние процессы, включая системы данных, применение оценки воздействия защиты данных и внутреннюю документацию для того, чтобы обеспечить полное соответствие с принципами GDPR.

Мы применяем технические и организационные меры для обеспечения защиты данных по умолчанию. Мы пересмотрели политику конфиденциальности и использования Cookies для наших потребителей, а также формулировку соглашений на обработку данных и различные независимые процессы, требующие прямого согласия пользователя на рекламные рассылки. Мы

используем прозрачную и понятную систему оповещений, предлагающую опцию отказаться от подписки на любые рекламные материалы.

Мы всегда проводим оценку воздействия защиты данных в случаях, когда их обработка идет в крупных объемах, несет высокий риск для прав и свобод граждан, или включает данные специальных категорий или информацию, связанную с уголовными обвинительными приговорами и правонарушениями. Для того, чтобы проводить оценку меры воздействия защиты данных в полном соответствии с требованиями GDPR, мы разработали специальные процедуры оценки риска при обработке данных, и применяем меры для уменьшения риска со стороны субъектов данных.

Мы не занимаемся целенаправленным сбором и обработкой персональных данных специальных категорий. Мы предупреждаем наших пользователей в политике конфиденциальности о том, что им не следует делиться такой информацией при использовании наших продуктов и услуг.

Мы предоставляем доступные сервисы поддержки. Наши сотрудники всегда рады помочь пользователям в защите их личных прав. Мы рассматриваем и исполняем запросы пользователей, касающиеся их прав на перенос, доступ, исправление и удаление данных. Мы также помогаем в защите других прав субъектов данных, изложенных в GDPR (например, право на возражение против обработки данных с целью прямого маркетинга в случаях его применения).