



Freiburg, May 14th 2025

## Russia moves to punish German company for providing Delta Chat

On May 14th, the Moscow City Court sided with Russian security authorities in ruling against merlinux GmbH in Freiburg for non-compliance to hand over user data and decryption keys of [Delta Chat](#) users. The latest court decision marks the end of a legal process that the Russian surveillance authority, Roskomnadzor, had started in July 2024, demanding access to user data and encryption keys from the German company that develops the email based encrypted instant messenger. “We can not hand out data that we don’t have,” says merlinux’s managing director Holger Krekel. “Delta Chat is an encrypted instant messenger app that works with thousands of user-chosen email servers without us knowing anything about their addresses or messages.”

Delta Chat apps gained popularity in Russia because of growing distrust of Telegram co-operating with Russian authorities, but also because the apps work decentralized and provide [security-audited end-to-end encryption](#). Russian YouTubers are lately giving Delta Chat increased attention (see for example <https://youtu.be/gT38FfOXv1E> ) also because the apps are [increasingly recognized as easy to use](#). “The precise usage numbers in Russia, however, remain unknown due to the technical architecture of how Delta Chat operates and because its developers deliberately avoid having any user data whatsoever,” notes [Ksenia Ermoshina](#), researcher at the French National Center for Scientific Research (CNRS) in Paris.

After the Moscow City Court decision, Russian authorities might take steps to block Delta Chat apps from being used in Russia. Recently [Apple removed VPN apps for Russian users](#) but so far has stayed clear of trying to remove instant messengers from app stores. However, in 2024 the [Signal messenger servers were blocked on the network level in Russia](#) along with Threema, SimpleX Chat and Matrix which can now only be used through network proxies or VPNs. “Delta Chat is not immune to blocking but it’s more resilient because you can not easily block all email servers without impacting business and government communication,” says Ermoshina, who extensively studied blocking attempts against messenger services in Eastern Europe, as well as the [re-routing of Internet traffic to Russian providers in the Crimean peninsula](#).

The Freiburg company is now planning to ask the UN Human Rights Committee to consider the lack of proper reasoning apparent in the Russian court procedures. “No state should strive for, or be allowed to demand breaking end-to-end encryption from application developers,” opines Krekel, who co-ordinates Delta Chat developments since 2017. “It is concerning that also in the EU there is a constant push towards breaking end-to-end encryption which is the bedrock of privacy in the Internet Age,” Ermoshina adds. “It is on the EU now to decide if they want to follow Russia’s example of demanding to break end-to-end encryption and ending what little is left of online privacy,” referring to the “ChatControl” plans in the EU to access citizen’s private communications.

### Contacts:

Holger Krekel: [holger@deltachat.de](mailto:holger@deltachat.de)

Ksenia Ermoshina: [ksenia.ermoshina@cnrs.fr](mailto:ksenia.ermoshina@cnrs.fr)

**Note: the following pages contain more legal and procedural details**



## Details about the court process which concluded on May 14th

**July 8th, 2024**, merlinux had received a notification of the initiation of administrative proceedings under Part 1 of Article 13.31 of the Code of Administrative Offenses of the Russian Federation. The proceedings concern the alleged failure to submit a notification of the commencement of activities related to the operation of information systems and/or software used for receiving, transmitting, delivering, and/or processing electronic messages of Internet users. FSB Order No. 432 of July 19, 2016, establishes that an Organizer of Information Dissemination on the Internet (OIDI) must provide decryption keys and related data within ten days of receiving a request from an authorized security agency. Merlinux explained at the time that the requirements to provide encryption keys and decrypt user messages in Delta Chat are technically infeasible and [contradict international standards](#) in the fields of [human rights and information security](#).

**August 13, 2024**, Roskomnadzor imposed a minimum fine of 100,000 rubles, claiming they were merely fulfilling the FSB's directive—disregarding both the factual context and the technical impossibility of compliance. Subsequently, merlinux's lawyers filed a complaint with the Simonovsky District Court of Moscow (<https://mos-gorsud.ru/rs/simonovskij/services/cases/appeal-admin/details/93202c00-660a-11ef-bdfe-35e810f03126?participant=merlinux>), arguing that the company is technically unable to comply with the FSB's requirements due to the architectural design of Delta Chat: the application vendor does not store user data and has no access to user messages, as the application operates without proprietary servers. At the court hearing, a representative of the Federal Security Bureau (FSB) —who had issued the non-compliance notice under Article 10.1 of the Information Law — testified that Delta Chat qualifies as an OIDI solely because it has a Russian-language forum where users communicate, and includes the ability to exchange electronic messages over the Internet. Despite the weak match of this argument with the actual operations of Delta Chat messenger apps (they do not depend on any forum software) this position was echoed by the Roskomnadzor representative, who emphasized that their agency was only enforcing the FSB's demands. The court accepted these arguments and, on **October 28, 2024**, dismissed the complaint of the German company.

Merlinux's lawyers then filed a complaint to the Moscow City Court. The details of the legal arguments for the **May 14th decision** can be found here: <https://mos-gorsud.ru/mgs/services/cases/review-not-yet/details/51d4c730-f861-11ef-ad21-077a437bc876?participant=Merlinux+GmbH>

Merlinux's lawyers specifically argued that there was a lack of technical expert examination which would have validated its position that the demand is technically infeasible. Russian law stipulates that an organization can be held liable only if it had the capability to comply with the law. In the case of Delta Chat such a capability does not exist. The administrative penalty was imposed for refusing to facilitate FSB access to confidential private information, amounting to interference with freedom of information and penalizing merlinux for adherence to international encryption and data protection standards.

Russian government order no. 743 of 31 July 2014 and the Ministry of Digital Development and Communications order no. 571 of 29 October 2018 mandate that a so called "OIDI" must install



equipment which is capable of searching, processing and delivering to the FSB the user identities and contents of messages, including necessary decryption keys. "It is obvious that we have no ability to install any such equipment at the email providers that Delta Chat users choose without our knowledge. We also have no access to encryption keys that would be needed to decrypt user data passing through those servers," explains Krekel. The Russian authorities suggest in their court arguments that merlinux could change the apps to introduce a back channel, and give the FSB access to it. "That would kill the whole purpose of providing a scalable end-to-end encrypted messenger with users choosing a server themselves," says Krekel.