

Newsletter

New legislative changes in the IT sector in June 2024

2 July 2024

Dear Ladies and Gentlemen!

We would like to inform you about the adoption of a new law that simplifies the procedure for blocking 'mirrors' of blocked websites, as well as new restrictions related to the use of foreign information security services.

Federal law on blocking 'mirror' websites

On 22 June 2024, Federal Law No. 158-FZ (the "**Law**") was adopted¹, which transfers the power to declare a website a 'mirror' of a pirate resource directly to the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (**Roskomnadzor**) by amending Article 15.6-1 of Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection" dated 27 July 2006 (the "**Information Law**").

Currently, the Information Law envisages the following procedure:

- ① Information about a copy of the blocked website is sent to the Ministry of Digital Development. Within one day, a decision is made to deem the resource a 'mirror', a copy of which is sent to the owner of the website and to Roskomnadzor;
- ② Roskomnadzor must inform hosting providers, telecommunications service providers and search engine operators within one day. Upon receiving information from Roskomnadzor, hosting providers, telecommunications service providers and search engine operators must restrict access to the 'mirror' website within one day.

Once the provisions of the new Law come into force, **the Ministry of Digital Development's powers will be transferred to Roskomnadzor**, thereby reducing the time required to restrict access to 'mirrors' of blocked websites.

The Law also expands the scope of legislation with respect to search engine operators by amending the Law on Information and Federal Law No. 236-FZ dated 21 June 2021 "On the Activities of Foreign Entities in the Internet Information and Telecommunication Network on the Territory of the Russian Federation" (the "**Landing Law**").

- ⬇ Before the Law enters into force, the obligations arising from having the status of a search engine operator were imposed on operators that **distribute advertising targeted at Russian consumers**.

As such, search engine operators that have ceased to distribute advertising but continue to operate in the Russian segment of the Internet are exempt from regulation.

Under the Landing Law, search engine operators are obliged to place disclaimers stating that the company to which a link is displayed in a search engine is not 'landed' and violates Russian law, and they must also remove such companies from the display.



The **amendments extend the existing obligations**, in particular the obligation to cease issuing information about a 'mirror' website in the search output and information about users when executing the 'right to be forgotten', as well as to inform users of violations and stop search results for companies that violate the Landing

¹ Federal Law No. 158-FZ dated 22 June 2024 "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and Articles 11 and 15 of the Federal Law "On the Activities of Foreign Entities in the Internet Information and Telecommunications Network on the Territory of the Russian Federation".

Law, to all search engine operators, regardless of whether they distribute advertising aimed at users in Russia.

The provisions of the Law expanding the definition of search engine operator would enter into force from the date of publication (22 June 2024), while the other changes would come into force from 1 October 2024.

Prohibition of foreign information security services from 'unfriendly' jurisdictions

On 1 May 2022, Presidential Decree No. 250 "On Additional Measures to Ensure the Information Security of the Russian Federation" was issued to impose new restrictions related to the use of foreign information protection tools for the Russian authorities, state corporations, systemically important organizations and subjects of critical information infrastructure ("**CII subjects**") from 1 January 2025. This includes a ban on the use of:

- Information protection tools **originating from 'unfriendly' states**²;
- Information protection tools that are **manufactured by organizations under the jurisdiction of 'unfriendly' states**, directly or indirectly controlled by them or affiliated with them.



On 13 June 2024, Presidential Decree No. 500 extended the scope of the ban: from 1 January 2025, **the purchase of information protection services** (work) from 'unfriendly' states **is now also prohibited**.

If your company is a CII subject, to ensure timely compliance with the requirements of the above-mentioned Presidential Decrees, we recommend conducting an audit of the software and IT services your company uses with the assistance of IT specialists.

The amendments also require the Federal Security Service (FSB) to establish requirements for accredited centres to be involved in incident response, as well as the grounds for the suspension and withdrawal of accreditation of these centres. CII subjects are required to notify the FSB about any information security incidents without delay. For this purpose, CII subjects should exclusively work with organizations accredited within the State System for the Detection, Prevention and Elimination of Consequences of Computer Attacks (GosSOPKA).

We hope that you find the information provided in this newsletter useful. If any of your colleagues would also like to receive our newsletters, please send them a [link](#) to the electronic subscription form. If you would like to learn more about our [Data Protection and Cybersecurity practice](#), please write back to us. We will be happy to send you our materials.

Note: Please note that all information has been taken from public sources. The author of this letter, as well as ALRUD Law Firm, is not responsible for any consequences resulting from decisions based on this information.

If you have any questions, please contact ALRUD Partner

Sincerely,
ALRUD Law Firm



**Maria
Ostashenko**

Partner

Commercial, Intellectual
Property, Data Protection and
Cybersecurity

E: mostashenko@alrud.com

² The list of 'unfriendly' states is defined by Order No. 430-p of the Government of the Russian Federation dated 5 March 2022.