



seamless  
LEGAL

DIGEST

# DIGITAL LAW

## From the authors

The concept of “digital law” is still a debatable issue. It is premature to speak of an independent and established branch of digital law. Nevertheless, for certainty, we will allow ourselves the following definition, which is established in the doctrine<sup>1</sup>.

Digital law is a system of rules of conduct that develops in the field of application or through the application of digital technologies and regulates relations arising in connection with using digital data and applying digital technologies.

We are pleased to present this digest for 2023 collecting the latest news in digital law. We believe that the digest encompasses all the main developments on the subject.

We hope you will find this information useful. Please feel free to contact us should you have any questions or suggestions!

Yours sincerely,

SEAMLESS Legal



**Vladislav Eltovskiy**

Counsel, Head of Digital Law

**T** +7 495 786 40 90

**E** [vladislav.eltovskiy@seamless.legal](mailto:vladislav.eltovskiy@seamless.legal)



**Shermet Kurbanov**

Associate

**T** +7 495 786 40 18

**E** [shermet.kurbanov@seamless.legal](mailto:shermet.kurbanov@seamless.legal)



**Elizaveta Isaeva**

Paralegal

**T** +7 495 786 41 71

**E** [elizaveta.tsurkan@seamless.legal](mailto:elizaveta.tsurkan@seamless.legal)

---

<sup>1</sup> Definition in the authors' abridged version. A full definition is provided in the following source: Digital Law: textbook / Under the general editorship of V.V. Blazheyev, M.A. Yegorova. - Moscow: Prospekt, 2020.

## Contents

What's new in biometrics? .....	4
Personal data: the latest developments .....	6
Recommendation algorithms: has it become more difficult to recommend?.....	10
New authentication and hosting rules.....	11
Advertising: labelling online advertising, fines and more .....	13
Foreign messengers are banned, and online resources are controlled .....	17
The rouble has found a new form: launch of the digital rouble .....	21
IT companies and Russian software .....	22
What's new in e-commerce: fifth antimonopoly package, marketplaces and digital signature.....	25
Changes in telecommunications .....	28
Fresh National State Standards (GOSTs) .....	29
New experimental legal regimes .....	30
Businesses will be restricted from using foreign words.....	32
Appendix 1.....	34
Appendix 2.....	37

## What's new in biometrics?

### Unified Biometric System

From 1 June 2023, a prohibition on processing specific biometric personal data outside the Unified Biometric System (the “**UBS**”) came into force. This has affected the ability of commercial organisations to process certain types of biometric data.

The UBS was created pursuant to [Law](#) No. 572<sup>2</sup>, which also regulates the identification and authentication procedures by means of biometric personal data.

The UBS currently includes the following types of biometrics: (a) an image of a person and (b) a record of a person's voice. This list may be extended after 1 September 2024.

Companies can now identify and authenticate individuals based on biometrics only through the UBS or accredited organisations, but only in the event that the individuals in question have given their voluntary consent.

A number of regulations on certain UBS issues have also been adopted in pursuance of the UBS law. For example, the [procedure and rules](#) have been established for the accreditation of commercial biometric systems (CBS), as well as the grounds for its suspension and termination. The full list of the regulations can be found in [Appendix 1](#).



More details on this innovation can be found in our alert: [Unified Biometric System: New rules for processing biometrics](#).

### Use of biometrics in individual cases

#### ***Fan ID Card***

On 15 March 2023, the Russian Government [Decree](#) came into force, allowing fans to obtain remotely a personalised card for attending a sporting event (Fan ID). They can also be identified using the UBS.

#### ***Biometrics in education***

As a general [rule](#), educational organisations cannot use biometrics to authenticate students.

The exemption is introduced from September 2024 for using biometrics in distance learning. The Government has [established](#) that the use of biometrics is authorised for identifying and authenticating students for assessment and ongoing monitoring.

---

<sup>2</sup> Federal Law No. 572-FZ dated 29 December 2022 “On Identification and/or Authentication of Individuals Using Biometric Personal Data, on Amending Certain Russian Laws and Repealing Certain Provisions of Russian Laws”

## Fines

On 12 December 2023, new fines were [introduced](#) for law violation when placing and updating biometrics within the UBS<sup>3</sup>.

The amendments address liability for law violation where banks, multifunctional centres and other organisations place and update biometrics within the UBS.

The fines for such a violation will range from RUB 100,000 to RUB 300,000 for officials and from RUB 500,000 to RUB 1m for legal entities.

---

<sup>3</sup> Federal Law No. 589-FZ dated 12 December 2023 "On Amending the Russian Code of Administrative Offences"

## Personal data: the latest developments

### Cross-border data transfer

On 1 March 2023, [amendments](#) to the Personal Data Law<sup>4</sup> came into force, relating to the cross-border transfer of personal data.



More details on all the amendments can be found in our alert: [Personal Data: major changes in the regulation](#).

We also recommend that you pay attention to the guideline “[How to correctly file a notification of cross-border data transfer](#)”, which Roskomnadzor issued in August 2023.

### **Requirements applicable to cross-border transfers**

The revised Personal Data Law tightens the rules for cross-border transfers. Before transferring personal data, companies will now have to:

- carry out an assessment of the recipient of the personal data located outside Russia;
- submit a notification to Roskomnadzor of their intention to transfer personal data outside Russia.

The further procedure depends on the country of the personal data recipient, namely whether this country is listed as a foreign state providing adequate protection of the rights of data subjects.

*For “adequate” countries.* Once the notification has been given, a company may immediately commence the cross-border transfer. Within ten business days, Roskomnadzor may decide to prohibit or restrict the transfer. In such a case, the data controller who transmitted the data must ensure that the recipient destroys the personal data.

*For “inadequate” countries.* After the notification has been given, a company may transfer personal data to the recipient only ten business days after Roskomnadzor receives the notification unless the latter has made a decision to prohibit or restrict the data transfer.

Roskomnadzor may extend the period for considering the notification by 15 business days when additional information is requested.

### **Bans and restrictions on the cross-border transfer of personal data**

In March 2023, decrees [No. 6](#) and [No. 24](#), setting out rules for making decisions to prohibit or restrict the cross-border transfer of personal data, came into force.

---

<sup>4</sup> Federal Law No. 266-FZ dated 14 July 2022 “On Amending the Federal Law “On Personal Data”, Certain Russian Laws and Repealing Article 30(14) of the Federal Law ‘On Banks and Banking’”

Upon considering a data controller's notification, Roskomnadzor may decide to prohibit the transfer of personal data in the following cases:

- the recipient of the personal data does not implement data protection measures or does not specify conditions for discontinuing their processing;
- the recipient of the personal data is an organisation whose activities are banned, or that is deemed "undesirable" in Russia;
- the transfer of personal data abroad and their further processing are incompatible with the purposes for which the personal data has been collected; or
- there are no legal grounds to transfer the personal data abroad.

Roskomnadzor may additionally prohibit or restrict cross-border transfer at any time by notice at the request of other supervisory authorities in order to protect the constitutional order, security, ensure defence and protect the national economic and financial interests.

If the underlying reasons cease to be in effect, Roskomnadzor may lift the ban or restriction on the cross-border transfer based on another submission by the relevant authority or a request from the controller whose data transfer was banned.



More details on the bans and restrictions can be found in our alert: [How can the cross-border transfer of personal data be banned.](#)

## Personal data destruction

Data controllers are required to document personal data destruction by signing an act in paper or electronic form<sup>5</sup>.

## Personal data leaks

### ***New powers of Roskomnadzor***

On 14 February 2023, Russian Government [Decree](#) No. 161 came into force, giving Roskomnadzor new powers. In coordination with the prosecutor's office, it is now authorised to conduct unscheduled inspections of accredited IT companies in 2023-2024 if they are found to be leaking personal data.

### ***Interaction with Roskomnadzor***

On 1 March 2023, Roskomnadzor [Order](#) No. 187 came into force, defining the procedure and conditions for interaction between data controllers and Roskomnadzor as part of keeping records of leaks.

---

<sup>5</sup> Roskomnadzor Order No. 179 dated 28 October 2022 "On the approval of requirements for confirming personal data destruction"

The Order details the content of primary and supplementary notifications, how and where the notification should be sent, and the procedure to be followed by Roskomnadzor in the event of non-receipt of the notification.

### ***Interaction with the Federal Security Service***

On 1 March 2023, Federal Security Service [Order](#) No. 77 came into force, defining the procedure for controllers to interact with the State System of Detection, Prevention and Elimination of Computer Attack Consequences where computer incidents are detected.

According to the Order, interaction in this case shall be carried out through the National Coordinating Centre for Computer Incidents (NCCCI).

Controllers that are subjects of critical information infrastructure that have established their interaction with the NCCCI<sup>6</sup>, shall report on any computer incidents to the NCCCI within 24 hours upon detection.

Other controllers shall report such incidents to Roskomnadzor via its website within 24 hours of the detection of an incident. They shall notify Roskomnadzor of the results of their internal investigation within 72 hours of the incident being detected. Subsequently, Roskomnadzor shall transmit such information to the NCCCI.

### ***Changes in the form of the Roskomnadzor check list***

On 16 April 2023, [amendments](#) to Roskomnadzor Order No. 253<sup>7</sup> entered into force, establishing the form of the checklist used by the authority in the exercise of its control and supervisory powers.

Adjustments are limited to modifying existing points and adding new points to the check list form.

## **Forms of notifications to Roskomnadzor**

Roskomnadzor [Order](#) No. 180 came into force at the end of 2022. The order establishes the forms of the following notifications:

- on the intention to process personal data;
- on the change of information contained in the notice of intention to process personal data;
- on termination of personal data processing.

---

<sup>6</sup> The National Coordinating Centre for Computer Incidents.

<sup>7</sup> Roskomnadzor Order No. 253 dated 24 December 2021 "On approval of the form of the check list (list of questions, answers to which indicate whether a controlled person complies or fails to comply with mandatory requirements) used in exercising federal state control (supervision) over the processing of personal data by the Federal Service for Supervision over Communications, Information Technology and Mass Media and its local offices"



## Fines

On 12 December 2023, [amendments](#) were made to the Russian Code of Administrative Offences increasing fines for personal data processing without the data subject's written consent, if required by law, or for failing to comply with the requirements for the content of the said written consent.


### *First violation*

<b>Category</b>	<b>Before</b>	<b>After</b>
Officials	RUB 20,000 – 40,000	RUB 100,000 – 300,000
Legal entity	RUB 30,000 – 50,000	RUB 300,000 – 700,000

### *Repeated violation*

<b>Category</b>	<b>Before</b>	<b>After</b>
Officials	RUB 40,000 – 100,000	RUB 300,000 – 500,000
Individual entrepreneur	RUB 100,000 – 300,000	RUB 500,000 – 1m
Legal entity	RUB 300,000 – 500,000	RUB 1m – 1.5m

## Recommendation algorithms: has it become more difficult to recommend?

From 1 October 2023, owners of websites, apps and software with recommendation  functionality must comply with new rules (we also covered them in our alert: [Online recommendation services to be regulated in Russia](#)).

The new regulation affects all online resources that provide information based on the collection and analysis of Russian users' preferences. This may include video services, e-book shops, social networks, e-commerce platforms and any other resources that promote content or goods on the basis of user preferences.

### What are the new responsibilities?

According to the [amendments](#) to the Law on Information, the obligations of owners of recommendation systems will now include:

- avoiding the use of recommendation technologies that violate the rights and interests of individuals and organisations or provide information prohibited by Russian law;
- informing users about the use of recommendation systems, and posting the owner's details and email address; and
- publishing rules on the use of recommendation technologies in the Russian language. The rules must contain a description of the processes and methods used in the recommendation system as well as the types of information collected.

### What liability arises?

In case of violation of these obligations, Roskomnadzor may issue a request for rectification. Failure to comply with the request may result in the restriction of access to the website in Russia.

To date, there are no fines for non-compliance, but these may be introduced in the future following an assessment of law enforcement practices.


Explaining the new provisions, Roskomnadzor presented an information [statement](#) "On the Application of Recommendation Technologies".

Also, from 12 December 2023, Roskomnadzor Orders [No. 149](#) and [No. 150](#) shall apply, establishing:

- requirements for the content of information on applied recommendation technologies and for placement of such information on a resource;
- the procedure for interaction between Roskomnadzor and owners of resources where recommendation technologies are used.

## New authentication and hosting rules

### “Authentication Law”: changes in the rules for user registration on Russian websites

From 1 December 2023, [amendments](#) to the Law on Information came into force concerning  user registration on Russian websites (we also covered them in our alert: [“Authentication Law”: new rules for user registration on Russian websites](#)).

According to the amendments, authorisation of Russian users online (on websites, in information systems and programmes) owned by Russian entities will be possible in one of the following ways:

- by phone via the user’s phone number of a Russian telecom companies;
- via the “Gosuslugi” web portal (the Unified Identification and Authentication System);
- through the Unified Biometric System;
- through other information systems owned by a Russian entity (without foreign control).

As yet, there is no liability for non-compliance with the new requirements, but there will likely be changes in terms of fines once the application of the new rules is assessed.

The new [law](#) dated 12 December 2023 provides for a transitional period until 1 January 2025 for the new authentication rules.

During this period, a Russian entity (website owner) may also use other information systems to authenticate Russian users provided that such systems meet (1) the information protection requirements (Article 16 of the Law on Information) and (2) the requirements for the owner of the other information system.

### New regulation of hosting providers

 From 1 December 2023, hosting providers have new responsibilities (we also covered them in our alert: [Hosting providers: new rules of operation in Russia](#)).

According to [amendments](#) to the Law on Information, hosting providers are required to:

- submit a notification on the commencement of their activities to Roskomnadzor (Roskomnadzor will maintain a register of hosting providers based on these notifications);
- ensure the protection of information within their infrastructure;
- cooperate with law enforcement agencies to provide information in the course of their investigative activities;

- participate in exercises to ensure a “Sovereign” Internet, install technical means to maintain it, and follow instructions as part of the centralised management of the Russian national segment of the Internet; and
- implement user identification/authentication procedures.

After 1 February 2024, individuals or entities not included in the register are prohibited from offering hosting services.

Furthermore, as of 1 September 2024, state and municipal information system operators will only be allowed to use hosting services from providers that are not under foreign control and have established technical hosting facilities within Russia.

The following regulations have been adopted in furtherance of the new hosting rules:

1.	Russian Government <a href="#">Decree</a> No. 1952 dated 22 November 2023	Rules of interaction of hosting providers with authorised state bodies carrying out operational and investigative activities or ensuring security of the Russian Federation
2.	Russian Government <a href="#">Decree</a> No. 1970 dated 23 November 2023	Criteria for involvement in formation and maintenance of the register of hosting providers
3.	Russian Government <a href="#">Decree</a> No. 2011 dated 29 November 2023	Rules for identifying and authenticating customers of hosting providers
4.	Russian Government <a href="#">Decree</a> No. 2009 dated 28 November 2023	Rules for a hosting provider to submit a notification to Roskomnadzor
5.	Russian Government <a href="#">Decree</a> No. 2008 dated 28 November 2023	Rules for forming and maintaining the register of hosting providers

## Restrictions for foreign hosting providers

Previously, the “Landing Law”<sup>8</sup> has established special rules for foreign entities whose activities are aimed at Russia, including foreign hosting providers, to carry out their online activities. Such entities are required to place on their resource a feedback form for Russian persons, register a user account on Roskomnadzor’s website, and open their branch, representative office or subsidiary in Russia. Foreign hosting providers are also obliged to comply with these rules.

It was due to non-compliance with these requirements that on 26 September 2023, Roskomnadzor adopted a [resolution](#) on enforcement action against 12 foreign hosting providers, including Amazon Web Services and GoDaddy. Search engines are now obliged to inform Internet users about companies failing to comply with Russian law.

<sup>8</sup> Federal Law No. 236-FZ dated 1 July 2021 “On the Online Activities of Foreign Entities in Russia”

# Advertising: labelling online advertising, fines and more

## Labelling of online advertising and new fines

In September 2022, the [requirements](#) for labelling online advertising came into force (as described in more detail in our alert: [Online advertising: new rules from 1 September 2022](#)). They include three main obligations:



- labelling advertising with the word “Advertisement” and stating information about the advertiser;
- placing a token (a unique identifier issued by an advertising data operator) on the advertising;
- reporting on online advertising to Roskomnadzor through the advertising data operator.

In October 2023, Roskomnadzor, together with the Association for the Development of Interactive Advertising (ADIR), issued an updated 6th edition of its [clarifications](#) on the procedure for accounting for online advertisements.

Also, in October 2023, Roskomnadzor issued its guideline “[5 steps to account for online advertising](#)”.

In November 2023, Roskomnadzor issued a memo, “Recommendations for placing an advertisement identifier”, to help market participants comply with the legal requirements for accounting for online advertising.

## Penalties for non-compliance with requirements on labelling online advertising

Liability for non-compliance with the requirement to label advertising with the word “Advertisement” and state information about the advertiser was already provided in Article 14.3(1) of the Russian Code of Administrative Offences. Compliance with these requirements is monitored by Russia’s FAS.

Regarding the token and reporting requirements, the liability was introduced on 24 June 2023,<sup>9</sup> and a new set of offences in the Russian Code of Administrative Offences came into force on 1 September 2023. The following fines currently apply:

---

<sup>9</sup> Federal Law No. 274-FZ dated 24 June 2023 “On Amending the Russian Code of Administrative Offences”

Offence	Fines
Lack of the word “Advertisement” and/or information about the advertiser or its website	<ul style="list-style-type: none"> <li>from RUB 4,000 to RUB 20,000 for company officers</li> <li>from RUB 100,000 to RUB 500,000 for legal entities</li> </ul>
Failure to fulfil the obligation to provide Roskomnadzor with information on advertising disseminated on the Internet	<ul style="list-style-type: none"> <li>from RUB 30,000 to RUB 100,000 for company officers</li> <li>from RUB 200,000 to RUB 500,000 for legal entities</li> </ul>
Failure to fulfil the obligation to place a token	<ul style="list-style-type: none"> <li>from RUB 100,000 to RUB 200,000 for company officers</li> <li>from RUB 200,000 to RUB 500,000 for legal entities</li> </ul>
Failure to fulfil the responsibilities of an advertising data operator	<ul style="list-style-type: none"> <li>from RUB 100,000 to RUB 200,000 for company officers</li> <li>from RUB 300,000 to RUB 700,000 for legal entities</li> </ul>

## Fines related to social advertising

On 17 February 2023, [Law](#) No. 32 came into force, establishing fines in relation to social advertising:

Offence	Fines
<ul style="list-style-type: none"> <li>Failure to provide the social advertising operator with information on the volumes, methods, forms and means of advertising dissemination and/or expected volumes of social advertising dissemination</li> <li>Failure to provide such information and/or expected volumes in compliance with the related</li> </ul>	<ul style="list-style-type: none"> <li>from RUB 30,000 to RUB 100,000 for company officers</li> <li>from RUB 200,000 to RUB 500,000 for legal entities</li> </ul>

---

requirements and requirements for the timing and procedure for such provision

---

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• Failure to enter into a contract with a social advertising operator for the dissemination of online social advertising</li><li>• Fee-based dissemination of the online social advertising provided by the social advertising operator on the basis of such a contract</li><li>• Allowing any form of restrictions on the social advertising operator when disseminating social advertising</li></ul> | <ul style="list-style-type: none"><li>• from RUB 30,000 to RUB 100,000 for company officers</li><li>• from RUB 200,000 to RUB 500,000 for legal entities</li></ul> |
| <ul style="list-style-type: none"><li>• Failure to notify the social advertising operator that the advertising system operator is allowed on the basis of a contract for online social advertising dissemination, to disseminate the advertising on an information resource owned by such advertising distributor.</li></ul>   | <ul style="list-style-type: none"><li>• from RUB 30,000 to RUB 100,000 for company officers</li><li>• from RUB 200,000 to RUB 500,000 for legal entities</li></ul> |
- 

## Advertising and the self-employed

On 1 August 2023, [amendments](#) to Article 8 of the Advertising Law<sup>10</sup> came into force.

Previously, only legal entities and individual entrepreneurs were required to indicate information about the seller in advertising any goods when selling them remotely. This obligation has now been extended to the self-employed. They have to disclose their full name and taxpayer identification number.

## Advertising of loans

On 23 October 2023, [amendments](#) to Article 28(3) of the Advertising Law came into force.

According to the amendments, if an advertisement for services related to granting, using and repaying a loan contains interest rate information, it must specify the ranges of values of the true interest cost. The font size for such information should not be smaller than that for the interest rate information.

The FAS has also posted its [clarifications](#) on these amendments.

---

<sup>10</sup> Federal Law No. 38-FZ dated 13 March 2006 "On Advertising"

## Advertising/non-advertising: FAS clarifies

On 14 November 2023, the FAS [published](#) the first part of its Guidelines clarifying the Advertising Law.

The Guidelines focus on the concept of advertising and include detailed comments from the FAS on the following issues:

- concept of advertising,
- (non-) limited scope of addressees of advertising,
- concept of the advertising object,
- sponsor advertising,
- social advertising,
- (non-) advertising from telecom operators,
- seamless integration and its criteria,
- print advertising,
- information in catalogues, on the seller's websites, in social media, in search results, in feedback, on users' personal pages.

On 28 December 2023, the FAS approved and published two new Guidelines from the series of clarifications of the Advertising Law (approved by the FAS' Order No. 1079/23 dated 28 December 2023):

- Guidelines on compliance with mandatory requirements “Requirements for advertising of certain types of goods” (alcoholic beverages, medicines and dietary supplements);
- Guidelines on certain issues of applying mandatory general requirements for advertising.

The FAS of Russia has issued cards on the distinction between advertising and information – a visual aid on what constitutes online advertising:

- [Part 1](#) | 14 September 2023 | Websites and social media of the manufacturer or seller of goods, marketplaces, topical blogs, feedback.
- [Part 2](#) | 22 September 2023 | Media, news and special interest communities, jobs, advertisements.
- [Part 3](#) | 2 September 2023 | Drawings in social media.



# Foreign messengers are banned, and online resources are controlled

## Ban on foreign messengers

On 1 March 2023, [Law](#) No. 584 came into force, amending the Law on Information.

The essence of the amendments boils down to prohibiting a certain category of entities (e.g., credit organisations or state-owned organisations) from using foreign messengers for:

- transferring payment documents;
- disclosing information that contains:
  - personal data of Russian citizens;
  - data on wire transfers;
  - information required to make payments, and/or information regarding accounts/deposits of Russian citizens.

It is also prohibited to connect any other systems to such messengers for wire transfer of funds of Russian citizens.

## Compiling a list of foreign messengers

Roskomnadzor [Order](#) No. 22 has approved a procedure for compiling and posting a list of foreign messengers on Roskomnadzor's website.

According to the order, Roskomnadzor shall compile the list electronically. It shall be compiled based on the results of analysing publicly available information posted online and information contained in the authority's information systems.

The [list](#) currently includes nine messengers: Discord, Microsoft Teams, Skype, Snapchat, Telegram, Threema, Viber, WhatsApp, and WeChat.

## Fines

On 24 June 2023, [amendments](#) to the Russian Code of Administrative Offences came into force, establishing fines for illegal use of foreign messengers. The fine ranges from RUB 30,000 to RUB 50,000 for company officers and from RUB 100,000 to RUB 700,000 for legal entities.

## New rules for placing classifieds

[Law](#) No. 584 mentioned above also sets out requirements for a classified service and new obligations for the owner of such a service.

According to the law, a classifieds service means an information resource used for interaction between users as part of placing various classifieds (for the sale of goods, exchange, provision of services, etc.), allowing users to set such classifieds on their own.

At the same time, the new rules apply to a service that is accessed by over 100,000 Russian users per day, and the service owner may be a Russian entity (without foreign control).

The owner of such a service shall, among other things:

- not allow the service to be used for illegal purposes;
- prevent the dissemination of defamatory or discriminatory information;
- specify on the service its e-mail address for sending legally significant communications, as well as its surname and initials or corporate name;
- install one of the computer programmes offered by Roskomnadzor to determine the number of users;
- ensure integration and interaction of the service with the Unified Identification and Authentication System and “Gosuslugi” under the rules established by the Russian Government.

Roskomnadzor is authorised to keep a register of such services and if information disseminated in violation of the law is found on a service, may apply to a court to restrict access to the service if its owner fails to comply with mandatory requirements.

The following regulations have been adopted in furtherance of the new rules:

1.	Russian Government <a href="#">Decree</a> No. 672 dated 28 April 2023	List of cases of integration of services with the Unified Identification and Authentication System and “Gosuslugi” and rules for such integration
2.	Russian Government <a href="#">Decree</a> No. 755 dated 16 May 2023	List of documents certifying that a service owner complies with the legal requirements, as well as the form and procedure for submitting such documents to Roskomnadzor
3.	Russian Government <a href="#">Decree</a> No. 757 dated 16 May 2023	Procedure for interaction between Roskomnadzor and a telecom operator or owner, and for restricting and resuming access to a service and notifying about such restriction
4.	Roskomnadzor <a href="#">Order</a> No. 27 dated 28 February 2023	Methodology for determining the number of information resource users per day

## New fines

### User count

On 17 February 2023, [Law](#) No. 32 came into force, establishing the liability of certain owners of information resources for failure to install a software programme to count the daily number of users. There are fines for offenders:

- for company officers – from RUB 30,000 to RUB 100,000;
- for legal entities – from RUB 100,000 to RUB 500,000.

### Social media

From 1 August 2023, [Law](#) No. 401 shall apply, laying down several offences for social media owners:

Offence	Fines
<ul style="list-style-type: none"> <li>• Failure to post an annual report on the results of considering appeals and social media monitoring</li> <li>• Failure to post the rules for using a social networking service and/or failure to inform about any changes in them</li> <li>• Failure to post an e-form for appeals</li> <li>• Failure to disclose information about the owner of a social networking service</li> <li>• Disclosing such information incompletely or inaccurately</li> </ul>	<ul style="list-style-type: none"> <li>• from RUB 200,000 to RUB 400,000 for company officers</li> <li>• from RUB 600,000 to RUB 1m for legal entities</li> </ul>
<ul style="list-style-type: none"> <li>• Failure to monitor a social networking service</li> <li>• Failure to take measures to restrict access to prohibited information</li> <li>• Failure to comply with Roskomnadzor request to lift measures restricting access to any information</li> </ul>	<ul style="list-style-type: none"> <li>• from RUB 200,000 to RUB 400,000 for company officers</li> <li>• from RUB 800,000 to RUB 4m for legal entities</li> </ul>
<ul style="list-style-type: none"> <li>• Failure to comply with Roskomnadzor's order to monitor a social networking service in order to identify information similar to that which such service's owner was obliged to remove on the basis of an earlier request/notice</li> </ul>	<ul style="list-style-type: none"> <li>• from RUB 500,000 to RUB 800,000 for company officers</li> <li>• from RUB 4m to RUB 6m for legal entities</li> </ul>

The law also provides for a set of offences applicable not only to social media owners but also to owners of news aggregators, audio-visual services and classifieds services.

Failure to provide or timely provide Roskomnadzor with data allowing to identify such entities is punishable by a fine for legal entities ranging from RUB 50,000 to RUB 300,000.

## The rouble has found a new form: launch of the digital rouble

On 24 July 2023, [Law](#) No. 340 was enacted, launching the digital rouble (as described in more detail in our alert: [The digital rouble: a new form of the national currency](#)). The main provisions of the law took effect on 1 August 2023.

The digital rouble is issued in addition to cash and non-cash roubles.

The CBR will become the operator of the digital rouble platform, an information system through which all digital rouble transactions will be conducted.

The CBR has been entrusted with ensuring the smooth functioning of the platform and will be responsible for opening digital accounts, conducting transactions with digital roubles, and other aspects of the platform's operation.

To fulfil its responsibilities, the CBR has adopted the digital rouble platform [rules](#) which set out requirements for banks, account types, information security requirements and other matters.

Users (individuals and companies) will interact with the digital rouble platform through platform participants, specifically banks.

In addition to Law No. 340 mentioned above, [amendments](#) to the Russian Civil Code have been adopted, classifying the digital rouble as a property right as being a type of non-cash funds.

In furtherance of the new law, the CBR has also adopted a number of regulations fully listed in [Appendix 2](#). Also, the CBR publishes documents relating to the digital rouble on its official [website](#).

## IT companies and Russian software

### Technology companies law

On 3 November 2023, a new [Law](#) No. 478 “On the Development of Technology Companies in Russia” came into force.

This law establishes the legal framework for the activities of technology companies, as well as state support measures for such companies.

A technology company is a Russian commercial organisation that develops or manufactures products (performs services or work) using innovative technologies.

For the development of and state support for small technology companies, a register is being created as part of the State Information System “Economy”. In order for a company to qualify as a small technology company, this register shall include information about it.

The law also regulates the activities of the Centre of expert examination of small technology companies when classifying a technology company as a small technology company.

The following regulations have been adopted in furtherance of the new law:

---

1.	Russian Government <a href="#">Decree</a> No. 1847 dated 2 November 2023	Rules for classifying and declassifying technology companies as small, rules for forming and maintaining a register of such companies, and a list of economic activities (under the National Classifier of Economic Activities) for such companies
2.	Russian Government <a href="#">Ordinance</a> No. 3051-r dated 31 October 2023	List of centres of expert examination of small technology companies
3.	<a href="#">Order</a> of the Russian Ministry of Economic Development No. 725 dated 20 October 2023	Procedure for determining fees for expert examination of small technology companies
4.	<a href="#">Order</a> of the Russian Ministry of Economic Development No. 726 dated 20 October 2023	Forms of an expert opinion on whether a technology company meets the criteria for a small technology company

---

## **Accreditation of IT companies and list of IT companies' activities**

On 22 February 2023, [amendments](#) were made to the Regulations on state accreditation of IT companies. Thanks to the amendments, more companies are now eligible for obtaining accreditation.

The amendments also establish that an IT company shall give consent to disclosing its tax secrets for a period of at least two years.

In addition, it will no longer be necessary to attach a CEO's non-conviction certificate for obtaining accreditation. Information will be requested directly from the Ministry of Internal Affairs.

Also, in August 2023, the Russian Ministry of Digital Development approved a [new list](#) of IT activities for the purposes of state accreditation of IT companies.

## **Incentives for IT companies and their employees**

### ***Exemption from VAT***

On 1 January 2023, [amendments](#) to the Russian Tax Code came into force, exempting from VAT the sale of exclusive rights and rights to use computer programmes and databases included in the unified register of the results of research, development and engineering of military, special or dual purpose.

### ***Deferment from conscription***

Pursuant to Russian Presidential [Decree](#) No. 660, from 1 January 2024, employees of accredited IT companies will be eligible for deferment from military service until they reach the age of 30.

### ***Preferential mortgage***

Pursuant to Russian Government [Decree](#) No. 1411, specialists working in the IT sector up to and including the age of 35 will be able to obtain a preferential mortgage loan at a rate of up to 5% per annum, without regard to salary requirements.

### ***Preferential loans***

Russian Government [Decree](#) No. 707 has simplified the conditions for lending to IT companies for implementing digital transformation projects.

In particular, now an accredited IT company does not have to meet the conditions required to be eligible for preferential tax rates or reduced tariffs for insurance contributions.

## Russian software

On 18 January 2023, the Ministry of Digital Development approved guidance [notes](#) on the transition to using Russian software, including at significant critical information infrastructure facilities, and on implementing measures aimed at accelerating transition of state authorities and organisations to using domestic software in Russia.

The notes contain recommendations for:

- structure, content of transition plans for the use of Russian software;
- time-frames for the transition to using Russian software;
- a list of organisational and technical measures to be implemented for the transition to using Russian software;
- the procedure for developing, coordinating, approving and implementing internal and external monitoring and control over the implementation of transition plans for the use of Russian software.

Support for Russian software shall also be provided at the regional level. In particular, [Law](#) of Moscow Region No. 46/2023-OZ dated 4 April 2023 provides that organisations may be eligible for a tax deduction where software from Moscow Region developers is installed, tested, adapted or modified.

## Moscow start-up register

Moscow Government [Decree](#) No. 700-PP has introduced a procedure for forming and maintaining a register of start-ups. It is placed on the portal <https://i.moscow/>.

A unified database of start-ups and technology companies has been created to facilitate access to regional support measures. Also, inclusion in the register will help obtain IT accreditation in a simplified procedure with the Russian Ministry of Digital Development.



# What's new in e-commerce: fifth antimonopoly package, marketplaces and digital signature

## Fifth antimonopoly package

On 1 September 2023, the so-called “fifth antimonopoly package” of [amendments](#) to the Competition Law<sup>11</sup> came into force after five years of discussions.

The amendments address, in particular, the regulation of companies’ activities on the Internet through digital platforms.

Specifically, the concept of the “network effect” is introduced to the antimonopoly legislation. This is when the value of a digital platform changes depending on the number of buyers and sellers on it. For example, the value of marketplaces or aggregators increases as the number of buyers and sellers using these platforms grows.

Now, in order to establish abuse of a dominant position by the owner of a digital platform, the antimonopoly authority must establish that the digital platform in question is subject to network effects.

In addition, [Law](#) No. 426 includes the use of digital algorithms in cartel agreements into the list of aggravating circumstances that are taken into account when imposing an administrative punishment.



More details on these innovations can be found in our alert: [Fifth antimonopoly package adopted](#)

## Good practices of interaction between marketplaces and right holders

On 17 July 2023, a non-profit partnership “Association of Corporate Lawyers”, with the participation of the Federal Antimonopoly Service of Russia, issued recommendations on identifying and dealing with counterfeit products.

The “[Good practices of marketplaces’ interaction with right holders and sellers as part of preventing the sale of counterfeit products](#)”, in particular, describe:

- a list of documents which a seller shall provide to the marketplace (and which, if suspected and upon request, can be provided to the right holder);
- signs that may increase the likelihood of the right holder discovering suspicious products on the marketplace;

---

<sup>11</sup> Federal Law No.135-FZ dated 26 July 2006 “On Protection of Competition”

- the procedure for responding to a complaint about suspicious products;
- cases of blocking a seller of goods (and not only its specific offerings of suspicious products) on the marketplace;
- certain acceptable and unacceptable practices of doing business and selling goods on marketplaces.

Also, in order to combat violations of intellectual property rights, marketplaces can exchange information through a unified information system implemented on the platform of the Association of E-commerce Companies so that other marketplaces can check infringing sellers of goods.

Open sources note that due to these recommendations, marketplaces blocked 2.4m counterfeit cards in 2023.

## Marking goods by marketplaces

On 1 March 2023, Russian Government Decree No. 1351 came into force, amending the Rules for marking light industry goods. Whereas previously, marketplaces were not participants in the circulation of marked goods, now, according to the amendments, they are obliged to report to the marking system on goods circulation and withdrawal from circulation.



More details on this innovation can be found in our alert: [Marking goods for marketplaces: changes from 1 March 2023](#)

## App store pre-installation

The Government has established [rules](#) for mandatory pre-installation of a unified app store on technically complex products.

Such a unified store shall be fully installed on a technical device either by the product manufacturer or by its authorised persons. The pre-installed store shall be free for consumers.

In addition, certain types of technically complex products shall have a pre-installed programme providing access to the Honest Sign System.

The new requirements for unified store pre-installation apply to devices manufactured after 30 November 2023.

## Pre-installation of other applications

Also, from 2024, there is a new mandatory list of programmes to be installed on certain devices before they can be sold to consumers. The document has retained the software from the previous list, except for Mail.ru News and OK Live for Android and iOS smartphones and tablets.



Also added to the new list are:

- Dzen and Rutube – for phones and tablets;
- Yandex Browser, AMEDIATEKA, KION, and several other programmes are for TV sets with the Smart TV function.

## **Changes in digital signature regulation**

On 4 August 2023, amendments were adopted to the Digital Signature Law , the main ones being as follows:

1. Now, if Russia has no international treaty, foreign digital signatures may be used on the basis of an agreement between participants in electronic interaction. Such signatures shall be recognised as valid provided that an accredited certification centre (or other entity established by law) confirms that the digital signature meets the requirements of such an agreement.
2. Digital signature keys shall be immediately eliminated upon the expiry of their validity periods.
3. Special rules are established for issuing an enhanced encrypted non-certified digital signature if an applicant reapplies to the same certification centre.
4. Certification centres have stopped issuing certificates with the details of a legal entity to its employees. Instead, from this period onwards, only an individual's certificate can be obtained, and a machine-readable power of attorney from the CEO can be attached when signing a document.
5. However, employees will be able to use their old valid certificates until 31 August 2024. In this case, a machine-readable power of attorney will not be required.
6. Financial market participants have been allowed to use machine-readable powers of attorney with the right of delegation.
7. The requirements for an accredited certification centre have become stricter.

## Changes in telecommunications

### Clarification of telecom operators' obligations

On 1 September 2023, [Law](#) No. 75 came into force, providing for a new obligation for telecom operators. Specifically, owners or other holders of technological communication networks that have an autonomous system number shall:

- store in Russia for three years any data on receiving, transmitting, delivering or processing of voice information, text messages, images, sounds, video or other messages, as well as user data;
- transfer this information to the authorities engaged in investigative activities or ensure Russia's security.

In furtherance of the new obligation:

- Russian Government [Decree](#) No. 1441, dated 1 September 2023, has established the rules for storing and providing this information to the investigative authorities.
- Russian Government [Decree](#) No. 1385, dated 29 October 2019, has established the rules for interaction between owners or other holders of technological communication networks and competent authorities.

### New fines

On 1 January 2024, [Law](#) No. 223 came into force, setting out new fines for telecom operators.

Specifically, for failure to comply with its obligation to implement the requirements for networks and means of communication used for investigative activities or ensuring national security, the operator may be fined from 0.1% to 0.3% of its proceeds from selling the goods (work, services) on whose market the violation was committed. The proceeds will be calculated for the year preceding the year in which the offence was detected or for a part of the year (preceding the date of detecting the offence) in which the offence was detected, but not less than RUB 1m.

Repeated commission of such an administrative offence is punishable by fines ranging from 1% to 3% of the proceeds but not less than RUB 1m.

## Fresh National State Standards (GOSTs)

During 2023, new cybersecurity GOSTs were adopted, which may be useful for IT companies:

1. [GOST R 59709-2022](#) “Information Protection. Computer Incident Management. Terms and Definitions”.

This document standardises defined terms in the field of computer attack detection, prevention and mitigation and computer incident response for their further use in developing national standards, regulations and guidance documents.

2. [GOST R 59710-2022](#) “Information Protection. Computer Incident Management. General”.

This standard defines the content of the following stages of computer incident management:

- organising computer incident management activities;
  - computer incident detection and registration;
  - computer incident response;
  - analysing the results of computer incident management activities.
3. [GOST R 59711-2022](#) “Information Protection. Computer Incident Management. Organising Computer Incident Management Activities”.

This standard defines the content of the steps in organising computer incident management activities, namely:

- developing a computer incident management policy;
  - developing a computer incident response plan;
  - designating a business unit responsible for computer incident management;
  - organising interaction with business units within the company and with external organisations;
  - equipment and material procurement for the business unit responsible for computer incident management;
  - organising training and awareness regarding computer incident management;
  - conducting drills to practice the activities under the computer incident response plan.
4. [GOST R 59712-2022](#) “Information Protection. Computer Incident Management. Computer Incident Response Guide”.

This document defines the content of the steps to be performed in such stages as:

- computer incident detection and registration;
- computer incident response;
- analysing the results of computer incident management activities.



## New experimental legal regimes

### New directions for experimental legal regimes (ELRs)

Russian Government [Decree](#) No. 281 has established that digital innovation ELRs may be established for the following areas of developing, testing and implementing digital innovations:

- “Telecommunications”;
- “Power sector”;
- “Processing of data, including personal data, and related activities”.

### ELRs in medicine and telemedicine

#### ***Telemedicine***

Russian Government [Decree](#) No. 1164 has established an ELR for medical activities, including based on telemedicine and technologies for collecting and processing information on the health and diagnoses of citizens.

This experiment started on 1 August 2023 and will last for three years. Its main objective is to expand the opportunities for a patient to receive consultations using telemedicine in routine medical care:

- where he/she refers to the disease (condition) diagnosed by a prescribing physician during a face-to-face appointment and
- if the treatment is continued at the patient’s choice by another physician of the same healthcare organisation with at least seven years of professional experience for the same disease (condition) where the prescribed treatment can be corrected or where treatment (if there was none) can be prescribed.

The experiment also provides opportunities for prescribing remote monitoring of a patient’s health based on the results of a consultation using telemedicine technologies.

#### ***Selling prescription drugs remotely***

Russian Government [Decree](#) No. 292 has established the procedure for conducting an experiment on the retail sale of prescription drugs remotely, and the requirements for participants in the experiment, trade procedure, delivery requirements and the procedure for issuing authorisations to participants.

The experiment will take place in Moscow, Moscow Region and Belgorod Region until spring 2026.

The experiment's main purpose is to work out the mechanism of remote trade in prescription drugs and then introduce such trade on a permanent basis.

For the purpose of this experiment, other regulations have also been enacted, establishing:

- [authority](#) of the Ministry of Health to provide methodological support for the experiment;
- [amendments](#) to the existing rules for authorising remote trade in drugs;
- [list](#) of medicines and pharmacotherapeutic groups of drugs authorised to be sold as part of the experiment.

### ***New regions in the ELR “Personal Medical Assistants”***

This ELR was introduced by the Russian Government's [Decree](#) No. 2276 back in late 2022. It aims to design, build and operate a Personal Medical Assistant platform through which the measurement values of special medical devices are received, processed, stored and transmitted to the systems of healthcare organisations.

When the experiment was launched, it applied to 6 Russian regions – Republic of Tatarstan, Magadan, Novosibirsk, Ryazan, Samara and Tyumen Regions.

Russian Government [Decree](#) No. 332 extends the experiment to Irkutsk Region and Khanty-Mansi Autonomous Area – Yugra.

### **ELR for agricultural drone operation**

Russian Government [Decree](#) No. 1510 has established an ELR for the operation of agricultural unmanned aerial vehicle systems.

The experiment started on 27 September 2023 and will also last for three years. The areas of development, testing and implementation under this ELR are:

- design, manufacture and operation of vehicles, including highly automated vehicles and civil unmanned aircraft;
- certification of operators, provision of transport and logistics services and organisation of transport services.

## Businesses will be restricted from using foreign words

On 28 February 2023, [amendments](#) to the State Language Law<sup>12</sup> came into force, restricting the use of foreign words in several key areas.

From then on, all companies operating in the Russian market shall comply with the new requirements for drawing up texts in a foreign language. Eventually, the use of foreign words that are not endorsed by official dictionaries may be banned.

The new version of the law provides for approving a list of so-called standard dictionaries, normative reference books and prescriptive grammars, which will enshrine the rules of the modern Russian language.

A similar list of dictionaries, reference books and grammars was previously approved by Order No. 195 of the Russian Ministry of Education and Science. Still, at that time, the legislation did not expressly require compliance with such rules. In light of the adopted amendments, the list is expected to be revised and approved by the Russian Government.

Once the list is approved, officers of commercial and non-commercial organisations will have to comply with the rules set out in relevant dictionaries, reference books, and grammar. In particular, the use of obscene language will be prohibited, as well as the use of any foreign loanwords that are not included in standard dictionaries as foreign words with no commonly used analogues in the Russian language.

In addition, amendments have been made to the law concerning the requirements for drawing up a text in Russian where it is given as a translation of a foreign text. The law previously contained the rule requiring that a text in a foreign language be accompanied by a Russian translation in the areas where the use of the Russian language is mandatory. Now, it specifies that such a text shall be equivalent in layout and technical design; namely, it shall be in the same colour, font type and size as the text in the foreign language.

The business areas affected by these innovations:

- advertising;
- mass media;
- cinemas;
- organising theatrical, cultural and entertainment events;
- education.

In addition, the law now includes two new provisions requiring that all organisations shall use the Russian language:

---

<sup>12</sup> Federal Law No. 53-FZ dated 1 June 2005 "On the State Language of Russia"



- in official dealings and correspondence with individuals;
- in information intended for consumers.

These rules actually extend the requirements of the law to companies in all areas of business and may apply to any information placed by companies on their websites or pages on social media, in correspondence with customers, on product packaging, etc.

It should be noted that the innovations will not affect the use of registered trademarks or trade names that are excluded from such regulation if expressly set out by the law.

At present, the legislation provides for no liability for failure to comply with the requirements of the law, nor does it designate a supervisory authority to monitor compliance with these rules.

Such rules are expected to be introduced into legislation once the list of standard dictionaries, reference books and grammars is approved.



More details on this innovation can be found in our alert: [Businesses will be restricted from using foreign words](#)

## Appendix 1

1.	Russian Government <a href="#">Decree</a> 359 dated 7 March 2023	Approves the rules for a UBS regional segment operator to provide the Russian Ministry of Internal Affairs and the Federal Security Service with information contained in the regional segment of the UBS
2.	Russian Government <a href="#">Decree</a> No. 810 dated 22 May 2023	Approves the procedure/rules for accreditation of commercial biometric systems (CBS), and the grounds for its suspension and termination
3.	Russian Government <a href="#">Decree</a> No. 815 dated 25 May 2023	Approves a blacklist for CBS and instances where biometrics can be used by organisations where consent to process such biometrics is given by means of a simple digital signature
4.	Russian Government <a href="#">Decree</a> No. 595 dated 14 April 2023	Updates the requirements for verifying simple digital signatures used to sign consents to the processing of personal data and biometric personal data
5.	Russian Government <a href="#">Decree</a> 893 dated 31 May 2023	From 1 September 2023, biometrics can be used in medical examinations using medical devices that provide automated remote transmission of information on the health of employees and remote monitoring of their health
6.	Russian Government <a href="#">Decree</a> No. 883 dated 31 May 2023	Approves the Regulations on the UBS and its regional segments
7.	Russian Government <a href="#">Decree</a> No. 851 dated 29 May 2023	Amends the rules for individuals to post their biometrics within the UBS
8.	Russian Government <a href="#">Decree</a> No. 670 dated 28 April 2023	Approves the procedure for the accreditation of state authorities and the Central Bank and the requirements for organisations engaged by these state authorities and the Central Bank to process biometrics
9.	Russian Government <a href="#">Decree</a> No. 585 dated 11 April 2023	Approves the regulations on federal state control (supervision) in the area of identification and/or authentication

10.	Russian Government <a href="#">Decree</a> 552 dated 6 April 2023	Approves the procedure and deadlines for considering an application for the formation of a regional segment within the UBS and for the deletion of a regional segment
11.	Russian Government <a href="#">Decree</a> No. 478 dated 27 March 2023	Establishes rules for an individual's dissent from collecting and placing their biometric personal data, revocation of such dissent and a multifunctional centre's written confirmation of the dissent/revocation, as well as forms for the dissent, revocation and written confirmation
12.	Russian Government <a href="#">Decree</a> No. 451 dated 24 March 2023	Approves the rules for requesting a UBS operator to provide information on the results of checking the conformity of biometric personal data provided
13.	Russian Government <a href="#">Decree</a> No. 405 dated 17 March 2023	Approves the rules for obtaining consent to the placement of biometrics in the regional segment of the UBS, as well as the form of such consent
14.	Russian Government <a href="#">Decree</a> No. 367 dated 9 March 2023	Giving the Ministry of Digital Development additional powers related to working with the Unified Biometric System
15.	Russian Government <a href="#">Decree</a> 1879 dated 21 October 2022	From 1 February 2023, an applicant can be authenticated in the Unified Identification and Authentication System using the Unified Biometric System in order to access information contained in the unified portal of public services
16.	Russian Government <a href="#">Ordinance</a> No. 207 dated 1 February 2023	Amendments to Russian Government Ordinance No. 1322-r dated 30 June 2018  Form of consent to personal data processing for registration in the Unified Identification and Authentication System and the UBS
17.	Russian Government <a href="#">Ordinance</a> No. 3375-r dated 28 November 2023	Approves the composition of the Coordination Council for developing digital technologies for identification and authentication based on biometric personal data
18.	<a href="#">Order</a> of the Ministry of Digital Development No. 446 dated 5 May 2023	Approves a list of security threats to commercial biometric systems (CBS)
19.	<a href="#">Order</a> of the Ministry of Digital Development No. 445 dated 5 May 2023	Approves a list of security threats to the Unified Biometric System (UBS)

20.	<a href="#">Order</a> of the Ministry of Digital Development No. 387 dated 20 April 2023	Approves business reputation requirements for the executive body and/or individuals-founders that hold over 10% of shares in CBS
21.	<a href="#">Order</a> of the Ministry of Digital Development No. 334 dated 31 March 2023	Approves the methodology for calculating fees for the use of the State Information System of the UBS, including its regional segments
22.	<a href="#">Order</a> of the Ministry of Digital Development No. 378 dated 17 April 2023	Approves the methodology for verifying the conformity of biometric data to UBS vectors
23.	<a href="#">Order</a> of the Ministry of Digital Development No. 432 dated 27 April 2023	Approves the procedure for the UBS operator to send its request to block, delete or destroy UBS vectors to the UBS regional segment operator, an accredited state authority, the Central Bank, or an organisation
24.	<a href="#">Order</a> of the Ministry of Digital Development No. 453 dated 12 May 2023	Approves the procedure for processing biometric personal data and vectors in the UBS and in the information systems of accredited state authorities, the Central Bank and a number of organisations
25.	<a href="#">Order</a> of the Ministry of Digital Development No. 658 dated 9 September 2022	Approves the standard procedure to be followed by multifunctional centre employees when placing and updating an individual's personal data for registration in the Unified Identification and Authentication System and when placing and processing biometrics
26.	<a href="#">Order</a> of the Ministry of Digital Development No. 848 dated 9 October 2023	Approves the procedure for the UBS operator to post on its official website the lists containing accredited state authorities, the Central Bank, CBS and other entities using the UBS and its regional segments
27.	<a href="#">Order</a> of the Ministry of Digital Development No. 1024 dated 29 November 2023	Approves the forms certifying that technologies for processing biometrics meet the requirements of the UBS law
28.	Bank of Russia's <a href="#">Directive</a> No. 6540-U dated 25 September 2023	Lists security threats in the interaction between financial market information systems and the UBS
29.	Bank of Russia's <a href="#">Directive</a> No. 6541-U dated 25 September 2023	Lists security threats in the interaction between CBS information systems and the UBS

## Appendix 2

---

1.	CBR <a href="#">Regulations</a> No. 820-P dated 3 August 2023 “On the Digital Rouble Platform”	Establish: <ul style="list-style-type: none"><li>• requirements for digital rouble platform participants and users</li><li>• types of digital rouble accounts</li><li>• procedure for providing access to the digital rouble platform</li><li>• types of and procedure for digital rouble transactions, as well as applicable forms of settlements</li><li>• procedure for the settlement of disputes and disagreements</li><li>• procedure for handling requests and claims from the digital rouble platform users</li><li>• procedure for control over compliance with the digital rouble platform rules</li><li>• procedure for interaction between the digital rouble platform and the CBR payment system</li></ul>
2.	<a href="#">Resolution</a> of the CBR Board of Directors dated 3 August 2023	The CBR has set tariffs for the digital platform operator’s services
3.	<a href="#">Album</a> of orders for the digital rouble platform	Defines the list and details of orders for digital rouble transactions, as well as the forms of such orders in electronic form and in hard copy
4.	<a href="#">Rules</a> for interaction between a financial intermediary and the CBR in managing cryptographic keys of the digital rouble platform	
5.	<a href="#">Rules</a> for operational and technical interaction between a financial intermediary and the CBR	

---

---

	when transacting on the digital rouble platform	
6.	CBDC. <a href="#">Standard</a> “Procedure for connecting a financial intermediary to the digital rouble platform”. Version 1.2	Defines the procedure for connecting a financial intermediary to the digital rouble platform and the procedure for its interaction with the Bank of Russia for the management of cryptographic keys
7.	Digital Rouble Platform Standard “Requirements and recommendations for user interfaces when transacting in the digital rouble”.  <a href="#">Version 1.0</a> (applied between 20 July 2023 and 9 January 2024)  <a href="#">Version 2.0</a> (applies from 10 January 2024)	Describes minimum requirements for user interfaces
8.	Digital Rouble Platform <a href="#">Standard</a> “Requirements for Operational and Technological Interaction on the Digital Rouble Platform”. Version 1.0	The Standard is an integral part of a digital rouble account agreement to be concluded between the digital rouble platform operator (the Bank of Russia) and credit institutions (digital rouble platform participants) and contains requirements for the procedure to be followed by digital rouble platform participants on this platform

---

