Russia

Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Kseniya Lopatkina, Vasilisa Strizh Kamil Sitdikov and Brian Zimbler

Morgan, Lewis & Bockius LLP

LEGAL AND REGULATORY FRAMEWORK

Government approach

1 | How can the government's attitude and approach to internet issues best be described?

The Russian authorities have shown substantial interest in the growth of the internet and online commerce, but legal developments in this area have been somewhat uneven. Recent new laws and regulations have sought to:

- strengthen controls over the content that is deemed harmful and empower the authorities to block non-compliant websites;
- require platforms that obtain personal data from Russian users or allow users to communicate with each other to store certain data locally in Russia and provide encryption keys to certain law enforcement authorities; and
- extend certain taxes, including value-added tax (VAT), to digital services and certain other online transactions.

While a number of these changes have drawn criticism and increased concerns about tighter regulation of the internet, official government policy is also committed to the development of the Russian economy through online commerce, among other key sectors.

Legislation

2 | What legislation governs business on the internet?

Generally, Russia has not yet developed detailed rules addressing online business. Provisions applicable to e-commerce may be found in many laws, including those governing contracts, consumer protection, advertising and communications, among others. The main Russian laws and regulations that are relevant to e-commerce include:

- the Civil Code of the Russian Federation (the Civil Code);
- Federal Law No. 126-FZ 'On Communications' dated 7 July 2003 (the Communications Law);
- Federal Law No. 149-FZ 'On Information, Information Technologies and Information Protection' dated 27 July 2006 (the Information Law);
- Federal Law No. 152-FZ 'On Personal Data' dated 27 July 2006 (the Personal Data Law);
- Federal Law No. 38-FZ 'On Advertising' dated 13 March 2006 (the Advertising Law);
- Federal Law No. 63-FZ 'On Electronic Signatures' dated 6 April 2011 (the e-Signature Law);
- Federal Law No. 161-FZ 'On National Payment System' dated 27 June 2011 (the National Payment System Law); and
- Law of the Russian Federation No. 2300-1 'On Protection of Consumers' Rights' dated 7 February 1992 (the Consumer Protection Law).

Regulatory bodies

3 | Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

There is no specific regulatory body responsible for regulation of e-commerce in Russia. However, state authorities in other areas regulate e-commerce to the extent the matter concerns their respective fields. For example:

- the Russian government (http://government.ru) is the main regulatory authority issuing various regulations in many areas of concern;
- the Federal Anti-monopoly Service of the Russian Federation (FAS) (http://fas.gov.ru/) regulates advertising and competition;
- the Russian Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing (Rospotrebnadzor) (https://rospotrebnadzor.ru/) regulates consumer protection;
- the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) (https://rkn.gov.ru) regulates personal data protection and the internet, including blocking access to websites with illegal content;
- the Russian Ministry of Communications (http://minsvyaz.ru/ru) is the principal regulatory body for the communications sector. It develops and implements state policy in the telecommunications sector and regulates internet access tariffs and charges; and
- the Central Bank of the Russian Federation (the Russian Central Bank) (http://www.cbr.ru/) regulates payments including using digital currencies.

Jurisdiction

4 | What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The key laws are the conflict of laws rules of the Civil Code and the jurisdictional rules of two statutes on litigation matters:

- the Arbitration Procedural Code if a matter relates to a dispute arising from commercial activities and involving legal entities or registered individual entrepreneurs; and
- the Civil Procedural Code if a dispute is of a non-commercial nature (eg, claims to block access to non-compliant websites) or

involves consumers or individuals other than registered individual entrepreneurs.

These rules are rather complex and must be reviewed on a case-by-case basis. With a few exceptions, the general rule is that parties to a cross-border trade contract are free to choose the governing law and dispute resolution procedure for their transaction. Generally, a Russian court will respect the parties' choice. Still, there are certain Russian law rules (mandatory rules) that will apply regardless of the laws the parties choose to govern their contract. For example, Russian consumer protection laws are among the mandatory rules. Further, in certain cases only a Russian court has jurisdiction over a dispute (eg, in consumer rights protection cases). If a contract has no dispute resolution clause or if a dispute does not relate to a contract, a Russian court may assert its jurisdiction even when the defendant is a non-Russian entity and sells goods online if, for example:

- the defendant has a Russian presence such as a Russian branch or representative office, or its management is located in Russia, or it has assets in Russia;
- a dispute relates to a contract performed or to be performed in Russia (eg, the goods are to be delivered to an address in Russia);
- a dispute relates to damages caused by an act or circumstance that occurred in Russia or to harm that occurred in Russia;
- a dispute relates to protection of the business reputation of a Russian-based claimant;
- a dispute relates to internet advertising directed at Russian consumers (this would be the case if, for example, an advertisement was in Russian, or was placed on a website located in the .ru zone); or
- a dispute relates to registration of domain names in the .ru zone or the provision of online services in Russia.

Establishing a business

5 | What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are no special rules for the establishment of digital businesses, so the general procedure applies. Generally, there are two ways of doing business with formal presence in Russia:

- setting up a Russian subsidiary; or
- establishing a Russian branch office of foreign company.

CONTRACTING ON THE INTERNET

Contract formation

6 | Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

In general, it is possible to form and conclude contracts electronically under the general rules of the Civil Code, for contracts to be formed in a simple written form. A simple written form is observed if a contract is entered into by exchanging correspondence including email, provided that it is possible to ascertain that a particular piece of correspondence originated from a particular party to the contract. For example, a simple written form is observed if the parties use e-signatures (see question 8). Further, a simple written form is observed and a contract is formed where a written offer to enter into the contract is accepted by the course of conduct (eg, by provision of services or payment within a time frame set by the offer). This rule is usually relied upon to support entering into 'click-wrap' contracts in Russia.

Notably, the Civil Code is amended with the effect from 1 October 2019 to provide that a simple written form is also observed if the electronic or other technical way of entering a contract allows:

- to reproduce the contract's contents on tangible media; and
- to reliably identify the contracting parties.

Applicable laws

7 | Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

There are no particular laws that specifically govern contracting on the internet or clearly distinguish between business-to-consumer and business-to-business contracts. Civil law rules on contracts will apply.

Generally speaking, these rules provide more protection to individual consumers (eg, an individual consumer may request in court to amend or terminate the contract if it contains obviously unfavourable terms and conditions for such consumer and he or she was not given sufficient opportunities to negotiate the terms and conditions of such contract if, for example, the consumer was given the form to sign). Further, Decree of the Government of the Russian Federation No. 612 'On Approval of the Rules for Remote Sale of Goods' dated 27 September 2007 which governs certain specifics of selling goods and services to consumers on the internet.

Electronic signatures

8 | How does the law recognise or define digital or e-signatures?

The Civil Code generally allows e-signatures. The e-Signature Law is the main law governing the use of e-signatures. It defines 'e-signature' as a piece of information in electronic form that is attached or otherwise related to another piece of information in electronic form (information that is to be signed by e-signature), and which is used to identify a person signing such piece of information. The e-Signature Law sets out three types of e-signatures:

- simple e-signature: a code, log-in, password (including via short message service), email, or any other means that the parties may agree as the means to confirm the fact of creation of an e-signature of the person;
- unqualified e-signature: a piece of information that is encrypted and requires an e-key to decode it. Similarly, to a simple signature, the unqualified signature is a means to confirm that a particular person has signed the document. In addition, this e-signature serves to ensure that no changes can be made in a document (information) after it has been signed; and
- qualified e-signature: this requires complex encrypting through cryptographic tools certified by the licensing and certification centre of the Russian Federal Security Service (FSB) (the list of currently certified tools is available at http://clsz.fsb.ru/certification.htm). To be decoded, it also requires an e-key. However, in contrast with the unqualified signature decoding key, this e-key is obtained by a holder of the qualified e-signature from an entity accredited as a 'certification centre' by the Ministry of Communications. The list of such centres is available at: http://minsvyaz.ru/ru/activity/govservices/certification_authority and includes both governmental authorities (eg, the Russian Tax Service) and private entities. A document signed with the qualified e-signature is equivalent to a wet-ink signed document. A document signed with a simple or unqualified e-signature is equivalent to a wet-ink signed document only if the law expressly contemplates so or if the parties to a wet-ink written agreement have agreed so.

Currently, e-signatures are used:

- to exchange data with state authorities (eg, making mandatory filings to tax authorities, state insurance funds or state statistical services or participating in electronic public procurement auctions and tenders);
- to sign accounting documents and tax returns;
- in banking business; and
- in transactions conducted via exchanges and in other areas.

Data retention

9 | Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

There are no particular data retention or software legacy requirements in relation to the formation of electronic contracts. General rules on retention of 'paper' documents including contracts will apply. For instance, Order of the Ministry of Culture of Russia No. 558 dated 25 August 2010 which lists documents that entities and state authorities usually retain and specifies a time period for storage of the documents. Generally, a 'paper' contract must be kept during the period when it is in force and for five years thereafter; the same rule should apply to e-contracts.

Breach

10 | Are any special remedies available for the breach of electronic contracts?

There are no special remedies available for the breach of electronic contracts, and the general rules of the Civil Code apply. For the business-to-customer contracts, the Consumer Protection Law provides additional remedy options (eg, fine for the failure to voluntary satisfy consumer's claim during the pre-trial procedure).

SECURITY

Security measures

11 | What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

Russian law does not prescribe the measures that companies or internet service providers (ISPs) must take to ensure the security of internet transactions. Generally speaking, encryption of e-contracts as such is not mandatory. However, companies and ISPs must take certain security measures if they process personal data. The Personal Data Law requires companies to take physical, technical and organisational security measures to minimise the risk of personal data made available to them (eg, during internet transactions) being destroyed or lost, accessed by unauthorised persons, processed unlawfully or in a way that is not compatible with the purposes for which it was collected, or modified because of unauthorised or unlawful actions. There exist rather detailed regulations on such security measures (including Decree of the Russian Federal Security Service No. 378 'On the Approval of Composition and Content of Organisational and Technical Measures on Personal Data Security during its Processing in Informational Systems with the Use of Cryptographic Protection Means Necessary for Compliance with the Protection Requirements with respect to each Protection Levels, as provided by the Russian government' dated 10 July 2014). In certain cases, encryption is mandatory (eg, when a data operator processes data of more than 100,000 non-employee individuals).

Government intervention and certification authorities

12 | As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

Yes, in certain instances. For example, under Russian law, 'information dissemination organisers' must provide Russian law enforcement authorities with decoding keys. An 'information dissemination organiser' is defined as a person operating information systems or programs for computers that are intended or used for the receipt, transmission, delivery or processing of electronic communications from internet users (in essence, any website or resource that allows users to communicate with each other can be viewed as an organiser). There are certification centres dealing with e-signatures (see question 8).

Electronic payments

13 | Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

The National Payment System Law regulates the use of electronic payment systems in Russia. It defines an electronic payment system as a system which allows a client to execute cashless payment using information technologies including payment cards and other technical devices. This Law also contains certain rules and restrictions on electronic payments (eg, individuals who are not properly identified for the anti-money laundering compliance purpose, are not allowed to make payments exceeding 15,000 roubles).

14 | Are there any rules or restrictions on the use of digital currencies?

The National Payment System Law regulates the use of digital currencies (notably, the definition of the digital currencies does not include cryptocurrencies, which remains a 'grey area'). This Law requires that only licensed by the Russian Central Bank credit organisations can be electronic payment system operators and process payments in digital currencies. This Law also prohibits providing loans in digital currencies.

DOMAIN NAMES

Registration procedures

15 | What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

Domain names are not intellectual property in Russia and may only be 'registered' and 'transferred' rather than 'licensed'. Russia-specific domain names are '.ru' and '.рф'. Rules for registration and use of '.ru' and '.рф' domain names are established by the non-commercial organisation Coordination Centre for TLD RU (see https://cctld.ru). Domain name registration is performed by registration agents accredited by the Coordination Centre. Domain names are attributed on a first-to-file basis for a period of one year and the term may be renewed annually. It is possible to register a '.ru' or a '.рф' domain name without being resident in Russia. There is a list of 'reserved domains' attributed by the Coordination Centre under special rules (eg, domain names for government needs such as 'gov.ru'; 'mil.ru'). Domain names may be transferred from one company or individual to another, subject to payment of a fee to a registration agent (registrar).

Rights

16 | Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

Under Russian law, domain names are not intellectual property and generally confer no additional rights. Russian law permits registration of a domain name as a trademark. Registration of a domain name that is identical or similar to a third-party trademark constitutes a trademark rights violation and an act of unfair competition, where there is a risk that consumers will be misled as to the identity of the business holding the given domain name.

Trademark ownership

17 | Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Russia is a first-to-file jurisdiction, which means trademark is protected upon its registration. Trademark registration is prerequisite to challenging a 'pirate' registration of a similar domain name if the website offers goods or services on the respective website similar to those covered by the trademark registration. Registration of a 'pirate' domain may be considered unfair competition if the website makes a false representation that the defendant is associated with the claimant and there is a likelihood of confusion.

Dispute resolution

18 | How are domain name disputes resolved in your jurisdiction?

There are no special rules for the domain name dispute resolution procedure. Disputes are resolved by:

- state commercial courts, if a dispute arises from commercial activities and involves legal entities or individual entrepreneurs; or
- courts of general jurisdiction, if a dispute is of a non-commercial nature or involves consumers or individuals other than individual entrepreneurs.

Arbitration is also possible (see question 55).

ADVERTISING

Regulation

19 | What rules govern advertising on the internet?

General rules on advertising apply to advertising on the internet. In addition, the Advertising Law contains special rules on advertising using telecommunications. The key rule is that, in general, distribution of any such advertising requires the prior consent of a person. A similar rule prohibiting mass dissemination of information without consent (anti-spam rule) is also contained in the Communications Law. The FAS has issued certain guidelines about advertising on the internet including a Letter 'On Advertising on the Internet' of 28 August 2015 (see https://fas.gov.ru/documents/575608). These rulings do not have the force of law but nevertheless are deemed authoritative.

Also, codes of conduct issued by various self-regulatory organisations contain non-binding guidelines on advertising in various areas. For example, the Russian Code 'On Advertising and Marketing Communications Practice' (see www.akarussia.ru/download/rrk.pdf) was created by a number of Russian non-governmental associations in 2012, and the FAS and a number of prominent industry players have endorsed it. Also, the Association of International Pharmaceutical Manufacturers (AIPM) has developed the AIPM Code of Practices (http://www.aipm.org/etics/) which provides ethical standards for areas of concern, including for promotion of pharmaceutical products on the internet.

Definition

20 | How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

Russian law does not have a specific definition of online advertising and the general rules on advertising apply. The Advertising Law generally defines 'advertisement' as any piece of information disseminated in any way, in any form and by using any means, addressed to an indefinite number of people and aimed at attracting attention to the object of advertising, forming or maintaining an interest in it and promoting it in the market. The FAS takes the position that any advertising that is placed on any website registered in the .su, .ru and .рф domain zones, as well as on any Russian-language page of any website registered in any other zone, is information intended for consumers in Russia, and hence is subject to Russian law (see the FAS Letter 'On the Latest Amendments to Requirements for Advertising Alcoholic Products' of 13 September 2012, at https://fas.gov.ru/documents/575766).

In sum, any information – including online editorial content – that meets the above criteria could be treated as advertising and caught by the rules on advertising. Note that the Advertising Law exempts certain information from the general rules on advertising, such as, references to products, manufacturers or sellers that are naturally integrated into works of science or literature.

Misleading advertising

21 | Are there rules against misleading online advertising?

Unfair or inaccurate (misleading) advertising is prohibited. The criteria of such advertising are listed in the Advertising Law, and include, among others:

- inappropriate (inaccurate) comparisons of the advertised goods with goods of other manufacturers or sellers. For example, the Russian Supreme Court has ruled that use of descriptions such as 'the best', 'first' and 'number one' is allowed only if it is accompanied by an indication of a specific criterion by which the comparison is made;
- inaccurate information on the advantages of the advertised goods against goods of other manufacturers or sellers; and
- any other inaccurate information on goods, including on their nature, composition, method and date of manufacture, purpose, qualities, conditions of use, place of origin, expiry dates and so on.

Advertising claims must describe the alleged violation, means, place and time of the advertising of concern and be supported by evidence. There are no industry-specific rules and the general rules of evidence will apply. For example, evidence could include screenshots of web pages certified by notary. There is no specific list of documents that advertisers have to keep on record.

Restrictions

22 | Are there any products or services that may not be advertised on the internet?

The Advertising Law lists goods and services that may not be advertised in any media, including on the internet. It includes goods whose production is prohibited under Russian law, such as:

- certain weapons;
- drugs;
- explosive materials;
- human body parts or tissue;

- goods subject to state registration in the absence of such registration (eg, unregistered medical devices);
- goods that require licensing or other permits in the absence of such permits (eg, insurance services provided by an unlicensed insurer);
- tobacco and tobacco products; and
- medical services for abortion.

Further, there are goods whose advertising is specifically prohibited on the internet (eg, alcoholic products).

In addition, there are goods and services for which advertising is restricted to certain websites. For instance, advertising of gambling and betting is allowed only on websites registered as Russian sport mass media, official websites of all-Russia sport federations or professional sports leagues, and websites owned by the founders of sport television (TV) channels.

Hosting liability

23 What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

The Advertising Law expressly contemplates the liability of advertising providers (ie, manufacturers, sellers and other persons that initiate the advertising), advertising producers and distributors. Usually, it is a monetary fine imposed on a company and its officers. Depending upon its role in the dissemination of advertising, a content provider can face liability as an advertising provider, producer or distributor.

There are no specific rules on ISPs' advertising-related liability; such liability should be determined on a case-by-case basis. For example, in certain cases, ISPs may be treated as advertising distributors and an ISP can be made liable for unsolicited advertising via telecommunication means. A domain administrator may face liability for distribution of inappropriate advertising on a website it administers.

FINANCIAL SERVICES

Regulation

24 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

There are special rules on the advertising and selling of financial services in general; these rules equally apply to internet transactions. In sum, only Russian-licensed financial institutions can be involved in these activities. The Advertising Law set out certain rules and restrictions for advertising of financial services.

DEFAMATION

ISP liability

25 Are ISPs liable for content displayed on their sites? How can ISPs limit or exclude liability?

ISPs can be held liable for intellectual property rights infringements with respect to the content displayed on their sites unless certain exemptions apply. In general, Russian law distinguishes three types of ISPs, as follows:

- persons performing 'transmission of materials' on the internet (eg, access providers);
- persons providing 'possibility to place materials' on the internet, or 'information required for obtaining such materials' (eg, website or platform operators); and
- persons providing 'possibility to access materials' placed on the internet (eg, hosting providers).

An access provider cannot be held liable for intellectual property rights infringements with respect to the content, if such provider:

- does not initiate the transmission of the allegedly infringing content;
- does not alter the allegedly infringing content (except for purely technical purposes); and
- is not and could not have been aware that use of the allegedly infringing content by the person initiating its transmission is illegal.

A website or platform operator cannot be held liable if it:

- is not and could not have been aware that use of the respective intellectual property in such content is allegedly illegal; and
- receives written notice of an infringement and expeditiously takes necessary and sufficient measures to remove the allegedly illegal content.

No similar exemptions exist for hosting providers, although arguably the same should apply.

Shutdown and takedown

26 Can an ISP shut down a web page containing defamatory material without court authorisation?

An ISP can shut down a web page with defamatory material without court authorisation if it is permitted by the terms of use offered to its users. Also, a web page must be shut down without court authorisation upon Roskomnadzor's request if it contains the following materials:

- information that shows disrespect to Russian governmental authorities, state symbols, or Russian society;
- information, which dissemination is restricted by Russian law (eg, calls to mass riot or extremist activity, child pornography and fake news); and
- mirror of the web page, access to which was previously restricted.

INTELLECTUAL PROPERTY

Third-party links, content and licences

27 Can a website owner link to third-party websites without permission?

Russian law does not explicitly require a website owner to seek permission to link to third-party websites. However, the website owner must carefully assess whether permission is needed as in some cases linking without permission may be viewed as copyright infringement (eg, when linking to a third-party website would be considered as unauthorised 'communication to the general public') or as an act of unfair competition (eg, if the content of the website contained insulting information about third-party goods or services), or dissemination of prohibited information (eg, if the website contains extremist materials).

28 Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

In most instances, a website owner cannot use third-party content on its website without permission. Third-party content will most likely be protected by copyright under Russian law. Thus, the use of third-party content on a website without the express authorisation (consent) of its owner will likely result in both civil and criminal liability. While Russia does not generally recognise the doctrine of 'fair use' of copyrightable

materials, the Civil Code allows the use of copyrightable materials without authorisation of the owner in limited cases for educational, scientific and similar purposes. Potential consequences for unauthorised use of third-party content include civil claims from content owners.

29 | Can a website owner exploit the software used for a website by licensing the software to third parties?

Yes, a website owner can exploit the software used for a website by licensing it to third parties so long as it is the owner of intellectual property rights associated with this software. If a website owner licenses the software from a third party, the scope of further exploitation of such software (including the right to sub-license it to third parties) depends on the scope of the initial licence.

30 | Are any liabilities incurred by links to third-party websites?

Russian law does not expressly regulate the use of third-party links. Depending on the circumstances of a particular case, a website owner that displays links to a third-party website may be held liable for unfair competition, copyright or other intellectual property (IP) rights infringement or other civil rights infringement. A website owner can also face criminal or administrative liability if the link directs to illegal content (eg, pornographic, violent or extremist content).

Video content

31 | Is video content online regulated in the same way as TV content or is there a separate regime?

There are certain rules that apply to both online video content and TV content. These include Russian child protection laws that set out age-rating requirements and Russian counter-extremism laws that prohibit dissemination of extremist content. In addition, there are specific rules for prohibited TV content (eg, manufacturing or consuming drugs, explosive manufacturing instructions, information on the methods and tactics of counterterrorist operations, information on children suffering abuse, among others). From 1 July 2017, similar, albeit not identical, restrictions apply to content distributed via online video services.

IP rights enforcement and remedies

32 | Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

In general, upon receiving a claim from an IP rights holder, the police may carry out a dawn raid of the infringer's premises and seize counterfeit goods. In addition, as part of the injunctive relief, a court may issue freezing injunctions with respect to equipment, materials or certain activities conducted on the internet, in the event such equipment, materials or activities are suspected to be infringe third-party IP rights.

33 | What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Under the Civil Code, civil remedies generally available to IP owners include cessation of IP infringement, recovery of losses (damages) or payment of statutory compensation, seizure of counterfeit goods, publication of the court's decision on the infringement indicating the actual rights holder and freezing injunctions.

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

34 | How does the law in your jurisdiction define 'personal data'?

The Personal Data Law is the main law governing personal data in Russia. Personal data is defined as any information directly or indirectly related to an identified or an identifiable individual (a personal data subject). All personal data is divided into the following categories:

- general data, which includes an individual's full name, passport details, profession and education, and any personal data other than sensitive or biometric data;
- sensitive data, which includes data relating to an individual's health, religious and philosophical beliefs, political opinions, intimate life, race, nationality and criminal records; and
- biometric personal data, which includes data such as fingerprints, iris images and, arguably, certain types of photographic images.

The processing of data in the categories in last two points above must be justified by reference to a specific purpose and, in most cases, requires an individual's explicit written consent.

Personal data can be processed without an individual's consent in the cases specified in the Personal Data Law (see question 37).

Registration requirements

35 | Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Under the Personal Data Law, a company or an individual that organises or carries out (alone or with other operators) the processing of personal data as well as determines the purpose, content and method of personal data processing is a 'data operator'. Website owners that collect personal data on their websites will be considered data operators.

A data operator must notify the Russian data protection authority, Roskomnadzor, before starting to process personal data (there are certain exceptions applicable for simple, one-off collections of data, non-automatic processing and HR-related data). This is a one-off notification and the data operator need not notify the authority of each instance of data processing. The data operator should amend the notification if the information contained in the initial notification changes. Roskomnadzor maintains a public register of data operators, based on the information contained in the notifications received (see https://pd.rkn.gov.ru/operators-registry/operators-list/). In the absence of any queries, Roskomnadzor acknowledges receipt of the notification and adds the information on the data operator to the register within 30 days of receipt of notification.

Under the Personal Data Law, the data operator must appoint a data protection officer. The officer must report directly to the general manager (director) and is responsible for the 'internal application of the provisions of the Personal Data Law' and other data-related laws, as well as for maintaining a register of data-processing operations. In particular, the officer must:

- implement appropriate internal controls over the processing activities of the data operator and its employees;
- make the data operator's employees aware of personal data-related regulations, any internal rules on data protection and other data protection requirements; and
- deal with applications and requests from individuals.

Cross-border issues

36 Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

The Personal Data Law does not specify its jurisdictional scope. It is generally understood that the Personal Data Law applies to any legal entity including any foreign entity with a legal presence in Russia that collects personal data in Russia. At the same time, under the Roskomnadzor interpretation, online businesses with no local presence may also be affected, particularly if they customise their websites for Russian users, have Russian versions of their website, place advertisements in the Russian language or deliver goods to Russia (see https://pd.rkn.gov.ru/docs/Kommentarij_242-FZ_final.docx). Among other things, they must comply with the 'local storage rule'. The local storage rule requires a data operator to ensure that the recording, systematisation, accumulation, storage, adjustment (update, modification) and extraction of Russian citizens' personal data is conducted using databases located in Russia.

The local storage rule does not restrict further transfer of Russian citizens' data to third parties located outside Russia. Once the personal data is collected in the primary database located in Russia, the data operator can transfer or provide access to the personal data or part thereof to a third party located outside Russia, provided that it has complied with the cross-border data transfer rules. For example, the data operator must check that the data subjects' rights are adequately protected in the foreign country before the transfer.

All countries that are party to the European Convention on Personal Data of 28 January 1981 are considered to be countries 'having adequate protection of data subjects' interests' (ie, 'safe' countries). Further, Roskomnadzor has approved the list of countries that are not party to the above European Convention but are, nonetheless, considered to be 'safe' countries for the purpose of cross-border transfers (including Canada, Israel, New Zealand, Mongolia and Peru; see https://pd.rkn.gov.ru/library/p193/p199/).

Cross-border transfers of personal data to 'safe' countries are not subject to any specific requirements, provided that the data operator has received consent from the data subject on the transfer of his or her data or the other legal grounds exist for such transfer. Data transfers to 'nonsafe' countries (eg, Japan and the United States) and in certain other cases are allowed only if the personal data subject has consented in writing to the cross-border transfer of his or her data or in certain other limited instances specified in the Personal Data Law.

Customer consent

37 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

As a general rule, the processing of personal data requires customer consent. There are 10 general exemptions from the consent requirement, including instances where data is processed to perform an agreement to which the individual is a party or under which the individual is a beneficiary or guarantor. Many online businesses use this mechanism to establish grounds for the processing of customers' personal data obtained through a website; the website's terms of use describe the processing of customer's personal data and serve as an agreement between the customer and the website owner.

Further, Russian law and court practice generally support the 'confirmed opt-in' concept in obtaining permission to process general personal data to send email communications. Explicit written consent is required in certain cases (see questions 34 and 36).

Sale of data to third parties

38 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

The Personal Data Law does not regulate the 'sale' of personal data. Any such 'sale' will be deemed a personal data transfer and will be subject to the rules and restrictions on data transfers. In many instances, transfer is not possible other than with a data subject's explicit consent. As a practical matter, any such sale will usually be documented as a provision of information services by the website owner to a third party.

Customer profiling

39 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

Currently, there is no law on profiling and the general personal data protection rules will apply. In sum, any data processing for the purpose of targeted advertising is allowed only with the prior consent of a data subject. See also question 14. The use of cookies is not clearly regulated by Russian law, and is currently considered by Roskomnadzor as processing of personal data and, arguably, may be considered legitimate only subject to the user's consent.

Data breach and cybersecurity

40 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

There are no rules specific to e-commerce and the general rules would apply. The Personal Data Law provides for obligations related to data security breaches. These include an obligation of a data operator to rectify any breach (including a security breach) within three days and to notify the affected individual within three days of the rectification. If a rectification is made at Roskomnadzor's request, the data operator must inform Roskomnadzor within three days of the rectification.

41 What precautionary measures should be taken to avoid data breaches and ensure cybersecurity?

A number of complex security requirements apply to data operators and third-party service providers that process personal data under the 'instructions of operator'. The Personal Data Law only refers to general principles of data security and does not contain any specific requirements. The Regulation of the Russian Government No. 1119 dated 1 November 2012 describes the organisational and technical measures and requirements that must be taken to prevent any unauthorised access to the personal data.

The data operator must take appropriate technical measures against the unauthorised and unlawful processing of data, as well as against accidental loss, blocking or destruction of processed data.

Insurance

42 Is cybersecurity insurance available and commonly purchased?

In general, Russian insurance companies offer cybersecurity insurance. However, it is not commonly used in commercial practice.

Right to be forgotten

43 | Does your jurisdiction recognise or regulate the 'right to be forgotten'?

The Information Law regulates the 'right to be forgotten'. Operators of internet search engines must, upon a request of an individual, 'deindex' articles containing information about the individual from their search engine if such information is untrue or outdated or has been illegally disseminated (few exceptions to the rule are available). If the operator fails to remove the data or provide a reason for refusal to do so, the individual requesting the deletion of information may file a court claim.

Email marketing

44 | What regulations and guidance are there for email and other distance marketing?

The rules on advertising using telecommunication means are set out in the Personal Data Law, the Advertising Law and the Communication Law. Generally, unsolicited advertising using telecommunication means (including email, fax or telephone) is prohibited. Any data processing for the purpose of direct marketing is allowed only with the consent of the data subject. Such consent can be revoked by the data subject at any time (see also question 19).

Consumer rights

45 | What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Under the Personal Data Law, an individual is entitled to request details of the processing of his or her data from the data operator and access his or her personal data. There is no statutory form for the request; however, the Personal Data Law requires that it contain information on the data subject's identity (ie, passport details of the data subject or his or her representative) and information necessary to find the appropriate records (ie, a detailed explanation of the relationship between the data subject and the data operator, including, for example, references to the relevant agreement or other arrangements).

If a data operator processes personal data of the data subject, the operator has 30 days to respond to the request of the data subject or his or her representative and provide the following information:

- confirmation of the processing of data;
- the legal grounds for and purposes of the processing;
- the purposes and methods of processing;
- the name and address of the data operator and any recipients (other than the data operator's employees) that have access to the personal data or to which the personal data may be disclosed under an agreement with the data operator or otherwise as required by law;
- the scope of the personal data processed and the source of the personal data (unless another procedure for receiving personal data is established by a federal law);
- the terms of processing, including the period for which the personal data will be stored;
- the scope of rights of the individual as provided by the Personal Data Law;
- information on any (implemented or planned) cross-border transfers of the personal data;
- if applicable, the name and address of any third-party processor of the personal data acting under instruction of the operator; and
- any other information as required by applicable law.

An individual may also request the correction of inaccurate data processed by the operator and require the operator to inform any third party that has access to the inaccurate data about the corrections made. Further, individuals are entitled to demand that the data operator discontinue processing the personal data (except where the processing cannot be terminated or where termination would result in violations of Russian law, eg, labour law requirements). Individuals can request the deletion of specific data if such data is inaccurate, has been unlawfully obtained or is unnecessary for the purpose of processing by the data operator.

An individual is generally entitled to compensation of losses as well as for any moral damage resulting from infringement of his or her rights related to personal data processing and protection.

Personal data laws extend to foreign individuals as well as Russian citizens. However, certain rules (eg, local storage requirements) only apply to the data of Russian citizens.

TAXATION

Online sales

46 | Is the sale of online products subject to taxation?

Yes. Under the Russian Tax Code, foreign companies that supply 'electronic services' to customers located in Russia must pay Russian VAT. 'Electronic services' include the sale of online products such as software, video games, e-books, music and films as well as other services provided online such as domain name registration, hosting, cloud storage, providing access to online search systems, advertising and certain other services. A customer is deemed to be located in Russia if any of the following criteria are met:

- the customer resides in Russia;
- the customer pays through a bank or electronic payment system located in Russia;
- the customer's IP address is in Russia; or
- the telephone number used for the purchase has the Russian country code (+7).

The rules apply to business-to-customer and business-to-business contracts.

Server placement

47 | What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

This is not clear. Russian tax laws do not specifically provide that the placing of a server by a foreign company in Russia creates a permanent establishment of such foreign company for tax purposes. However, there are some arguments to support the view that a local server should be treated similarly to a local warehouse and thus creates a permanent establishment if owned or leased by the foreign company.

Company registration

48 | When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

Foreign companies providing electronic services must register for VAT within 30 calendar days of the date on which they started providing electronic services to customers located in Russia. It is possible to register online through the designated portal of the Russian Federal Tax Service (https://lkioreg.nalog.ru/en). Domestic internet sales are taxed same as offline sales.

Returns

49 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

This will depend on the facts and circumstances of each particular transaction, as well as on the terms of a contract between the selling offshore company and the onshore retail store. Generally speaking, if the price returned to the onshore company is unreasonably higher than the costs paid by the customer to the offshore seller while purchasing the products online, transfer-pricing issues may arise. This is a complex issue that requires special tax advice in each particular case.

GAMBLING

Legality

50 Is it permissible to operate an online betting or gaming business from the jurisdiction?

No. Under Russian lottery and gaming laws, it is prohibited to organise and conduct games of chance using information systems, including the internet or mobile networks. Betting companies are not allowed to accept bets through money transfers except for 'interactive bets'. Interactive bets can be accepted and processed by Russian-licensed financial institutions only based on a contract with associations of betting companies.

51 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Online casinos and betting websites are not allowed in Russia. Offline casinos, betting companies and financial institutions processing 'interactive bets' (see question 50) are required to verify the identity and age of the players. The minimum age for participation in betting activities is 18 years.

OUTSOURCING

Key legal and tax issues

52 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

Legal and tax issues with respect to outsourcing of services depend on the nature of the service being outsourced. However, some of the issues are common for any services. These include, for example, issues related to personal data transfers between the customer and the provider and issues related to intellectual property rights in the results of the services. Further, Russian labour laws, generally, prohibit temporary staffing except in limited cases and through accredited employment agencies. Accordingly, outsourcing contracts should be drafted carefully to avoid the contract being viewed by the courts as illegal.

Employee rights

53 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, and do the rules apply to all employees within the jurisdiction?

Generally, there are no specific obligations of the employer and no specific employee rights in connection with the outsourcing of a service or business function. There are also no specific consultation or compensation rights set forth as a matter of Russian law. Under Russian law, outsourcing of a service or function is often structured as dismissal by the previous employer and hire by the new employer. Dismissal invokes certain employee protections. Some categories of employees are protected from dismissal at the employer's initiative, such as pregnant women and single parents with children below a certain age. Further, if a trade union is registered, consultations with trade union representatives could be required in case of dismissal of a trade union member.

ONLINE PUBLISHING

Content liability

54 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability? Is it required or advised to post any notices in this regard?

- A website provider is liable for the distribution of 'fake news'. Fake news is broadly defined as any unverified information that threatens someone's life or health or property, public peace or security, or threatens to interfere or disrupt critical infrastructure, transport or public services, banks, communication lines and facilities, power and industrial facilities.
- A news aggregator owner is an owner of a website or specific software that:
  - processes and distributes news information online in the Russian language;
  - can be used to publish advertisements; and
  - is accessed by more than 1 million users a day must check the accuracy of socially important information before its dissemination and immediately discontinue the dissemination upon receiving an order from the competent authority. A news aggregator owner should not be liable if such distributed information is a 'word-for-word reproduction of communications and materials or their fragments that have been distributed by mass media which can be located and held liable for violations of the Russian mass media legislation'.
- Additionally, liability might be assessed on a fact-based review depending on such content (eg, advertising, news information) and consequences (eg, defamation, IP breach). See also question 26.

Databases

55 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

Under Russian law, databases are copyright-protected. Data included in such databases can also be protected as a separate IP object (depending on its content).

The Information Law allows for 'out-of-court' and 'court' procedures for blocking access to content whose distribution violates third party IP rights.

In the out-of-court procedure, the rights holder (or exclusive licensee) may send notice of violation of its IP rights to the owner of the website on which the content is posted. Such notice must be accompanied by documents confirming the IP rights and describing the violation. Upon receipt of this documentation, the website owner may agree to delete the content.

In the court procedure, the rights holder must first obtain a court decision confirming that its IP has been illegally distributed (used) on website and can further apply to Roskomnadzor with a request to block access to the relevant website. Roskomnadzor will then order a hosting provider to restrict access to the illegal content and, if there is no

response from the hosting provider, will order a communication operator to do the same. The operator must restrict access to the particular content, but if this is not technically feasible, it must block the entire web page or even website. Using the court procedure, it is generally possible to block access to a website forever.

DISPUTE RESOLUTION

Venues

56 | Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts or other venues that deal with online/digital issues and disputes.

ADR

57 | What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

Online/digital disputes can be referred to commercial arbitration. Russian law allows both ad hoc and institutional arbitration. For domain name disputes, the Uniform Domain Name Dispute Resolution Policy may be used if parties expressly agree to it in a contract.

UPDATE AND TRENDS

Key developments of the past year

58 | Are there any emerging trends or hot topics in e-commerce regulation in the jurisdiction? Is there any pending legislation that is likely to have consequences for e-commerce and internet-related business?

The three key trends are as follows:

- The emerging of new types of media and internet services (online and electronic newspapers, blogs, social media, messaging apps, aggregators and services) that fall outside of traditional regulation attract attention from the government. This results in new regulation affecting these new types of media and services. For example, following the adoption of special regulation on virtual private networks, messengers and online cinemas in 2017, Russia introduced special rules for ecommerce platforms that aggregate information from online shops and service providers in 2018. In March 2019, Russia changed its Civil Code to include 'digital rights', and further laws regulating activities in this field are pending.
- Russia continues to strengthen the governmental control in the cyberspace to combat cybercrime. This resulted in adoption of Federal Law No. 187-FZ 'On the Security of Critical Information Infrastructure of the Russian Federation' dated 26 July 2017 in effect from 1 January 2018. Further, Russia has amended its main laws governing the internet to allow the government to restrict access to the internet and to control internet traffic in emergency situations. In particular, Federal Law No. 90-FZ dated 1 May 2019 introduced a set of amendments to the Communications Law and the Information Law. These amendments are colloquially referred to as the 'sovereign runet law' or the 'law on the secured internet'. Most of them are in effect from 1 November 2019.
- Russia continues to strengthen control over information posted online to prevent dissemination of information it deems harmful or illegal. For example, under Federal Law No. 31 of 18 March 2019, online media and communications services providers are required to prevent distribution of 'fake news'. Fake news is broadly defined as any unverified information that threatens someone's life or health or property, public peace or security, or threatens to interfere or disrupt critical infrastructure, transport or public services, banks, communication lines and facilities, power and industrial facilities. Also, Federal Law No. 30-FZ dated 18 March 2019 enabled Roskomnadzor to require deleting information that shows disrespect to Russian governmental authorities, state symbols, or Russian society, and to block non-compliant resources.

Morgan Lewis

Ksenia Andreeva
ksenia.andreeva@morganlewis.com

Anastasia Dergacheva
anastasia.dergacheva@morganlewis.com

Anastasia Kiseleva
anastasia.kiseleva@morganlewis.com

Kseniya Lopatkina
kseniya.lopatkina@morganlewis.com

Vasilisa Strizh
vasilisa.strizh@morganlewis.com

Kamil Sitdikov
kamil.sitdikov@morganlewis.com

Brian Zimbler
brian.zimbler@morganlewis.com

Legend Business Centre, Tsvetnoy Bulvar, 2
Moscow 127051
Russia
Tel: +7 495 212 2500
Fax: +7 495 212 2400
www.morganlewis.com