Technology M&A 2021

Contributing editors
Arlene Arin Hahn and Neeta Sahadev

LEXOLOGY
Getting The Deal Through

GDR

Publisher
Tom Barnes
tom.barnes@lbresearch.com

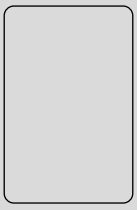
Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2018
Third edition
ISBN 978-1-83862-412-5

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112



Technology M&A
2021

Contributing editors
Arlene Arin Hahn and Neeta Sahadev
White & Case LLP

Lexology Getting The Deal Through is delighted to publish the third edition of *Technology M&A*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Russia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Arlene Arin Hahn and Neeta Sahadev of White & Case LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
October 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Russia

Alla Y Naglis and Xenia A Melkova
King & Spalding LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

Technology M&A deals in Russia are subject to numerous rules and restrictions. First, limitations on foreign investments are set with respect to Russian mass media (Mass Media Law 2124-1 of 27 December 1991) and online video-on-demand services that have substantial audiences in Russia (Information Law 149-FZ of 27 July 2006, as amended). A bill of law currently under consideration would similarly limit foreign participation in significant information resources (ie, major Russian IT companies) if approved.

Second, state approval is required for foreign investment in companies involved in certain types of activity of significance for the state under Law 57-FZ of 29 April 2008, as amended. The list of strategic activities includes:

- space-related activities;
- certain activities related to aviation and transportation security;
- certain biotechnology research;
- research involving nuclear materials;
- work and research in the military field;
- television and radio broadcasting (depending on the coverage);
- activities of a telecom operator with a dominant position on the market; and
- cryptography.

Applications for 'strategic investment' approvals are considered by a special governmental commission – a separate body that meets on an ad hoc basis to review such deals. Members of the commission include the prime minister, his or her deputies, other heads of state departments, and state agencies and services.

The above restrictions typically have the heaviest impact on a deal's structure. The approvals are commonly addressed in the definitive documentation as non-waivable conditions precedent to deal closing. In practice, these conditions are usually the last to be met and (with respect to the 'strategic investment' clearance in particular) may take months. Filings are done by buyers, subject to sellers' comprehensive support, and provision of documents and information.

Third, businesses in the technology sector may be subject to specific requirements of the Russian privacy statute (Personal Data Law 152-FZ of 27 July 2006, as amended), the statute on online payment services (National Payment System Law 161-FZ of 27 June 2011, as amended), the law on electronic signatures (E-signature Law 63-FZ of 6 April 2011, as amended), and certain provisions of the civil legislation concerning digital rights and assets, and e-commerce (Civil Code).

Lastly, Part IV of the Russian Civil Code, which governs intellectual property, applies in specific technology-related deals, including in relation to so-called 'integrated solutions'. An 'integrated solution' is the result of scientific and technological development that includes various combinations of IP that can be used for civil, military or dual purposes. These provisions apply to integrated solutions created with the use of federal or regional budget funds and specify when a Russia or a federal subject is recognised as the owner of the solution or has rights with respect to its exploitation. Further requirements for the disposal of integrated solutions owned by state or federal subjects, including the granting of rights to such solutions to third parties for implementation, are set forth in Law 284-FZ of 25 December 2008, as amended.

Certain limitations may be imposed by regulation in the sphere of secret protection, including, in particular, the State Secret Law (5485-1) of 21 July 1993, as amended. State secret requirements may apply to state-funded developments, including the integrated solutions described above.

Registration requirements that may affect the transfer of rights in M&A transactions are set for certain types of intellectual property by the relevant provisions of Part IV of the Civil Code.

Transfer limitations also exist for certain telecom and broadcasting licences (Communications Law 126-FZ of 7 July 2003, as amended, and the Mass Media Law, as well as ancillary licensing regulations).

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

Part IV of the Russian Civil Code provides for specific rules applicable to works of science, literature and art, inventions, utility models and industrials designs, selection inventions, and circuits created under state or municipal contracts. Unless otherwise specified in the relevant contracts, rights to such IP are retained by the authors or contractors. However, in any case where the state, federal subject or municipality is acting as the client, such a client has the reserved right to grant free non-exclusive licences in such IP to any party of their choice for the use of the IP for state or municipal purposes. The same rule applies to any software not specifically commissioned under a state or municipal contract, but created in the course of performance thereunder.

Specific rights can be vested with the state or federal subjects with respect to integrated solutions, including technology of civil, military or dual purpose, depending on certain criteria set forth in the Civil Code.

A number of major technology development projects are operated under the control of, or with the participation of, the state or the city of Moscow, including the Skolkovo Innovation Center and, notably, the artificial intelligence development experiment in Moscow, which began on 1 July 2020. In some of these projects the scope of state and municipal

rights to end products may be not evident, but should be subject to examination.

In addition, in practice the government has another efficient way to articulate its concerns and interests at the state approval procedure stage or antitrust clearance stage. While it is common for antitrust clearance to be conditional and involve a request that parties take certain steps aimed at mitigating potential negative impact on competition, until recently such conditions had not directly affected the technology aspects of the contemplated transactions. In April 2018, the Federal Antitrust Service of Russia (FAS) approved the merger of Bayer Germany and the US company Monsanto with respect to the Russian market, under the condition that Bayer share its selection technologies with Russia. Under the terms of the order issued by FAS along with the approval, Bayer agreed to hand over molecular markers for breeding of several types of crop, provide access to digital agriculture technologies and participate in the establishment of a local technology transfer centre. This was the first reported case where FAS made technology transfer of this scale a condition to deal approval in Russia. Thus, deal structuring should take into account the possibility that clearances may involve conditions, including the provision of access to production capacities or information, assignment or prohibition of assignment of property rights, and establishment of protection for industrial property.

Legal assets

3 How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

In the absence of specific regulation for many newer technologies, one of the main tasks in deal structuring is identifying all elements of the asset in question that can be protected by Russian legislation. For most types of technology, the key element is software, which is protected under copyright regulation. Other elements may include patentable designs or methods, databases, know-how or other protected IP.

Aside from IP legislation, Russian legislation does not contain specific provisions on the transfer of rights to technologies. The exception is the recently introduced provisions of the Civil Code on digital rights (in force since October 2019), which are not yet functional due to the absence of supporting laws and regulations. The new legislation is primarily designed to regulate token and cryptocurrency trade. The bill of law on digital assets is shortly expected to be signed into law that is designed to provide rules and regulations for trading processes and initial coin offerings. At the same time, approach to cryptocurrencies remains conservative and current initiatives tend to develop towards restrictions of turnover and extensive state control. Investments via online investment platforms (which may or may not be qualified as crowdfunding) are regulated under a separate law in force since January 2020.

The general rule is that a transfer of any IP asset that is subject to mandatory state registration is also registrable. Thus, patentable intellectual property (including inventions, utility models and designs) is registered with Rospatent, the federal authority for intellectual property; Rospatent also registers any disposal of patent rights.

Russia has no mandatory requirements for the registration or depositing of copyrightable works, but there is an option to register software (or databases) on the register operated by Rospatent, or on the register of Russian-made software managed by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. The latter register was created to support locally produced products and as part of software localisation requirements applicable to state-controlled companies.

Additional formalities may be applied to certain technologies or solutions that fall under state secrets, or other types of protected secret or confidentiality obligations. For example, a mandatory bid process is required for the disposal of state-owned integrated solutions; if a technology is protected by state secret, it is not accessible by, or allowed to be disclosed to, anyone who lacks the corresponding access rights.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Due diligence of a company with technology or IP assets usually involves the review of registrations for registrable IP rights, chain of title for copyrightable works (including software), review of IP assignment provisions in employment or similar contracts (if the company generates IP assets in-house or orders the development to third parties), and review of contracts for acquisition or licence of IP rights. In addition to the IP section, due diligence would also focus on relevant regulatory requirements and analysis of compliance therewith. Such regulatory requirements depend on the type of technology, but the critical provisions for which compliance should be checked are usually those under the personal data regulations and the requirements and limitations set forth under the Information Law 149-FZ of 27 July 2006, as amended.

It is also customary to review the history of claims, if any, over the relevant intellectual property or technology and, if the assets are licensed to third parties in the normal operations of the target, the actual licences would be reviewed.

In addition, due diligence may also include a review of a company's books to confirm if relevant IP and technology objects are adequately reflected as intangible assets. In some cases, such analysis reveals assets not otherwise disclosed by the target. However, such a review would rarely help with the determination of the value of technology and IP assets, as the valuation market for such assets is immature. If relevant assets are generated within the company or have never been transferred or licensed, their value in books can be arbitrary. The issue of the evaluation of technology and IP assets can be crucial in both share acquisition deals and asset purchases, when the share or asset price is tied to the book value.

Due diligence processes or potential carveouts or asset purchases do not involve in-depth review of the seller's corporate structure and potential corporate risks, as well as lending history and debts, but would rarely be notably different as regards the IP assets or technology.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

The official state register of registrable IP rights (eg, trademarks, and patentable inventions, designs and utility models) is available online on the website of the federal authority for intellectual property (Rospatent). The register enables users to confirm the ownership and any transfers, licences and encumbrances related to an asset. The same resource contains the register of voluntarily registered software programs and databases.

Ownership of domain names can be checked online in the WHOIS service database. For Russian domain names, information on the website administrator (if corporate) is often available, as well as the reference to the relevant local registrar.

Information on litigations, including the background of ongoing cases and, among others, bankruptcy cases, can be found online in the open register for disputes subject to consideration by the arbitration courts (ie, disputes involving commercial entities and business interests).

In any due diligence of a potential merger or share acquisition, the main source of corporate information is the Unified State Register of Legal Entities of Russia. An excerpt can be generated online and will show if the company is in the process of reorganisation or liquidation. For limited liability companies, the register also contains information on participants and their participation interests.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Under Russia's civil legislation, the rights to the following intellectual property are subject to mandatory state registration: trademarks, appellations of origin, inventions, utility models and industrial designs, and selection inventions. Software, databases and circuits may be registered at the right holder's discretion. Further disposal or encumbrance of rights to registered intellectual property is also subject to state registration. As from 27 July 2020, the Civil Code includes a new type of registrable intellectual property: geographical designation for marks identifying goods produced in specific regions.

Copyright and related rights are protected by Russian laws irrespective of registration. While software (which is protected as literary works) can be registered voluntarily, there are no state registers or depositories for other copyrightable works.

Domain names are not regarded as intellectual property, but they are protected as a means of use of registered trademarks and company or trade names. Rights to domain names are registered with the relevant national registrars acting under the general rules of Russia's Coordination Center for TLD RU. Information on registration can be checked in the Whois database available online.

Registrable rights are relatively easy to check in the course of a due diligence exercise, since most of the information is available in online state databases. Moreover, with respect to mandatory registrable types of intellectual property, the parties are entitled to rely on the information in such registers, which is why no further review is usually undertaken. Compared to registrable objects, rights to copyrightable works require more substantial revision of the underlying documents. Rights to such works are normally confirmed through establishing a proper chain of title, which may include licence or transfer agreements with previous owners, or employment or commissioning contracts with relevant authors. A review should confirm that relevant contracts are compliant with mandatory requirements of the legislation, that all conditions precedent to the transfer of rights were met by the purchaser, and that there are no terms allowing authors or previous rights holders to reverse the transfer of rights.

Importantly, the protection of certain types of intellectual property, even registrable, can be terminated in specific circumstances. Thus, trademark protection can be terminated if the owner fails to use the trademark for three consecutive years; and patent protection can be terminated if the patent fee is not paid within the set term. The risks of loss of protection are also analysed in due diligence.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Liens and security interests with respect to IP assets are allowed by Russian law, as long as the assets in question are transferrable – thus, moral rights, for example, cannot be encumbered. Encumbrances on registrable IP rights are also subject to mandatory registration with the state, which makes checking and confirming rather straightforward a task. For intellectual property not subject to registration, liens can be certified with a notary and entered into the register of notary notifications on liens, thus making this information presumed as available to third parties.

The law also requires that each pledgor keeps a pledge book as a company's internal document.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

In respect of employee-created works, the vesting of the rights in such intellectual property with the employer is rather straightforward. The Russian IP legislation contains specific provisions for the so-called 'employment works' – that is, works created by employees within their employment duties and job description. In such cases, employees retain non-proprietary moral rights, while the employer is granted exclusive proprietary rights to the works, unless the parties otherwise agree in the employment contract.

The practical application of the concept of 'employment work' entails some specificities. Thus, in order to qualify as such, the employment work must clearly and undoubtedly fall within the description of the employee's duties. In accordance with the explanation provided by the Plenum of the Supreme Court of Russia in its Ruling No 10 of 23 April 2019, if the status of the work is disputed, the employer has the burden of proving the scope of the employee's duties and the relevant work matching within such duties. The use of an employer's materials by an employee is not considered grounds for recognising his or her work as employment work.

Another issue is related to the fact that the Civil Code expressly states that the employee is entitled to compensation where the employer uses the employment work, licenses or assigns it, or even if the employer decides to keep such work a secret. While it is common practice to specify in the employment contract that any compensation for exploitation of employee-created works is included in the salary, some scholars opine that such provision is not sufficient and does not make the employer compliant with the legal requirement.

Lastly, if within three years of creation of the relevant work the employer neither commences the exploitation of the employment work, nor licenses or assigns it, nor notifies the author of the intention to keep the work a secret, the proprietary rights automatically return to the author.

Contractor-created works may fall into two categories: works specifically commissioned by the target and works created as a by-product of the provision of other works or services to the client. If the contractor was hired for the creation of intellectual property, the contract qualifies as authorship commission and, by default, vests the rights in the work with the client, unless otherwise agreed between the parties. In cases where creation of intellectual property is not within the main scope of the contract, the rights would normally be retained by the contractor. To avoid any risk of confusion, it is advisable to specify that the contractor undertakes to transfer any and all rights to the works or other IP results or technologies created in the course of the provision of services to the client, irrespective of whether such results were expressly commissioned.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

Under Russian law there are two categories of IP rights:

- Non-proprietary moral rights. These are non-transferrable and technically non-waivable by authors (inventors) together with some other specific rights such as the right of access or right to resale royalties.
- Proprietary rights (ie, the rights to exploit the intellectual property). These are defined in their entirety in respect of a particular intellectual property as the 'exclusive right'. A proprietary right can be assigned or licensed (in the latter case, as a whole or in parts). Unless the agreement expressly states that the entire 'exclusive right' is assigned, such agreement is presumed to be a licence.

The term used in Russian law for all proprietary rights – namely, 'exclusive rights' – is somewhat confusing and may erroneously be understood as referring to an exclusive licence. The law further distinguishes between exclusive and non-exclusive licences. Under a non-exclusive licence, the licensor retains the right to grant other licences, while an exclusive licence means that the licensor is not entitled to grant licences to other persons, or (unless the parties agree otherwise) to use the intellectual property itself. If there are no provisions on exclusivity, the licence is presumed to be non-exclusive.

Under a licence agreement, the proprietary right stays with the original rights holder, while certain rights and powers are granted to the licensee with respect to specific means of use, territory or term of use. The rights to use the intellectual property not expressly specified in the licence agreement are retained by the licensor. As the licensee does not own the proprietary right, the ownership of a licensed IP right cannot be assigned by the licensee. However, the licensee's rights may be transferrable if the licence agreement allows assignment or novation. Sublicences may also be granted by the licensee, if expressly allowed by the terms of the licence.

The owner of the proprietary right is not restricted by law from assigning its right, irrespective of whether it has been licensed to a third party. In case of such assignment, the licence remains valid.

There are specific requirements for licence agreements under Russian legislation, which are usually the subject of review during due diligence. To be valid, a licence agreement has to be concluded in writing. If a licence agreement contains no provisions on the territory and the term of use, the territory is presumed to be the territory of Russia and the term is presumed to be five years. Most importantly, a licence agreement must contain provisions on the licence fee. Free licensing is not allowed between commercial organisations worldwide for the entire term of use and on exclusive terms. If a non-free licence agreement contains no provisions on the amount of the fee or means to determine it, the agreement is considered non-existing.

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

Since software is protected by copyright as a literary work, due diligence typically includes the review of the underlying chain of title documents, such as employment or service contracts (if software was created in-house or commissioned), or licence or acquisition agreements (if the software was purchased or licensed from other parties). If the relevant software appears in one of the state registers, the information can be confirmed in the online database of the relevant registrar.

Legal due diligence does not typically include a review of the code itself, which can be done as part of a separate technical due diligence. There is no uniform approach to requesting code scans and, while buyers agree that full-scope due diligence and code analysis are preferable, whether a buyer insists on the review of the code as part of due diligence largely depends on the buyer's business (technology-related or investment) and the level of the buyer's technological savviness.

Other due diligence

11 What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

With respect to most new technologies, due diligence in Russia usually focuses on regulatory compliance and risks that may affect the exploitation of the relevant assets. Regulatory areas to look into may include personal data regulation and consumer protection, and regulation applicable to online payment systems, electronic signatures and the distribution of certain types of information.

Privacy issues emerge in nearly all new technology projects. Russian legislation uses a broad definition of 'personal data', understanding it as any information related to a directly or indirectly identified or identifiable individual. The authority responsible for supervising compliance with personal data protection requirements (the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Media) also tends to treat any type of data pertaining to an individual as personal data. The authority's approach to some of the interpretations of the legal provisions is not fixed in any official way and is often inconsistent, which makes it difficult to rely on. Different approaches to the legislation on big data have been discussed over the past few years. Various authorities are planning bills of law in this regard, with major industry players also involved (one of the bills suggested by the Ministry of Digital Development, Communications and Mass Media was rejected by the government in March 2020). Until changes are implemented, the competent Russian authorities are examining each case separately, but there have been situations when cookie files, IP addresses and online logs have been considered capable of identifying individuals and personal data. Consequently, any business plans involving the collection or transfer of data pertaining to Russian citizens should be analysed from the perspective of compliance with the Russian personal data regulation, including the requirements on data localisation.

Another specific consideration is the list of restrictions and requirements set by the Information Law 149-FZ of 27 July 2006, as amended, with respect to information distribution. The law contains specific requirements applicable to hosts of online platforms enabling the exchange of messages (including instant messaging services) to operators of search engines, news aggregator websites and video-on-demand services. Among such requirements are registration with state registers, mandatory identification of users, storage and the on-demand provision to state authorities of users' correspondence and metadata, and the provision of codes for deciphering transmitted data.

The absence of specific laws or legal provisions regulating technologies in such popular areas as artificial intelligence, the internet of things or autonomous driving does not mean the absence of regulation altogether. There may be certain requirements set at the authorities' level that are a challenge to track. For example, starting from January 2020 operators of low-power wide-area network (LPWAN) frequencies (normally used for the internet of things) are obliged to use base stations manufactured in Russia. The requirement was adopted by a decision of the State Radio Frequencies Commission in December 2018.

Many new technological projects are developed within the state's national programmes, such as the Digital Economy Programme. The

companies involved in these projects are acting under the approval and coordination of the state and within temporary requirements. One of such projects is the testing of autonomous cars in the territory of Moscow and the Republic of Tatarstan, rules for which were set in Governmental Order 1415 of 26 November 2018.

Under a law adopted in April 2020, starting from 1 July 2020 Moscow serves as a platform for an artificial intelligence development experiment. Entities and individuals involved in the experimental projects can benefit from a special regulation regime.

PURCHASE AGREEMENT

Representations and warranties

12 | In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

It would be fair to say that all technology M&A deals include some IP, technology, data privacy and security representations and warranties; however, the very concept of the representation or warranties may differ depending on the law governing the deal. In the authors' experience, English law-governed deals dominate the market, largely as a result of multi-level corporate structuring, with the target's and buyer's holding companies located outside Russia. English law agreements usually contain warranties.

If the deal is governed by Russian law, a somewhat similar concept of 'representations as to facts' recently introduced into Russian civil legislation can be used. The seller gives representations with respect to circumstances that are of importance for the execution, performance under or termination of the deal. In case the representations are not true, the seller is obliged to reimburse the buyer for all the damages caused by the breach of representation, and if the representations were substantial for the deal and the buyers' decision to enter into it, such party is entitled to terminate the agreement. The concept of 'representations' is actively used in Russian law-governed contracts; that said, since the concept's introduction in 2015 the courts' practice has not developed to allow adequate prediction of the outcome of disputes as the Russian legal system does not rely on precedents.

Regarding the scope of the warranties, in general, Russian sellers are more willing to give warranties with respect to shares and corporate status and would normally insist on qualifying and limiting warranties on compliance, tax and business. It is customary to include representations and warranties with respect to intellectual property and technology, which would normally cover ownership, validity and enforceability, no infringement of third parties' rights, no claims, validity of third-party licences, and similar. Specific warranties on open source code are increasingly often seen.

Cybersecurity warranties are not as typical, but if the main asset involves operation of networks or systems, it would be customary to request warranties concerning measures and security of these systems.

Data privacy is usually covered by warranties for general state requirements compliance, or separately as compliance with requirements for personal data protection.

It is customary to limit representations and warranties by seller's knowledge, or by referring to actual facts, rather than general compliance. For example, instead of confirming that the company complies with personal data protection requirements, the sellers would normally insist on warranting the absence of claims by the competent authority with respect to data processing within a certain period. For data security, it would be customary for sellers to warrant that the company does not install malware, rather than to confirm that the system is appropriately protected.

Customary ancillary agreements

13 | What types of ancillary agreements are customary in a carveout or asset sale?

In general, asset sales are less popular than company acquisitions, as the transferring of rights to registrable intellectual property and certain permits and licences for operation in different technology-related areas is time-consuming and complicated. In some cases, licences and permits are non-transferable. It is not uncommon for the seller to already have a separate business with related assets extracted in a separate company in the group. Using a company acquisition approach also helps to minimise transitional issues, especially for portfolio investors.

Buyers usually use a carveout approach for tax and regulatory compliance issues. In deals structured as carveouts or asset sales, service agreements and cross-licences are typical for transitional periods, with the asset support system remaining with the seller.

Conditions and covenants

14 | What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

For IP-focused deals, a chain of title corrections is a typical pre-closing condition, as well as requirements to complete registration of registrable intellectual property, and to clear any existing encumbrances and not create new ones. Pre-closing conditions may also require amendments to target's policies and templates, if IP and technology assets are created or supported in-house.

For post-closing covenants, there may be the seller's obligation to first offer new developed products (eg, software) to the buyer. Buyers also typically look for non-compete and non-solicit obligations, even though such provisions may be hard to enforce in Russia. In terms of intellectual property, the Russian Civil Code does not allow any limitations of the author's creative rights.

It is typical in Russian M&A deals to secure the seller's obligations by a performance guarantee issued by the seller's beneficial owners or the seller group holding company.

Survival period

15 | Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

Survival periods for IP representations and warranties are heavily negotiated and often tend to be shortened. In normal scenarios, such survival periods would coincide with those agreed for other representations and warranties, and rarely exceed one year for general warranties and three years for key assets.

Breach of representations and warranties

16 | Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

There is no typical approach to evaluating caps on liabilities for breach of IP representations and warranties. Normally, the parties' agreement depends on the asset and its value. Liability caps on IP warranties can be even lower than the caps for other representations and warranties, since the appropriate evaluation of these rights may be problematic.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

There is no market standard, and the parties may form their approach on a case-by-case basis. Same as with liability caps, parties are more likely to limit the scope of representations and warranties. Different types of intellectual property can have different thresholds and limitations, depending on how easy it is to trace risks and encumbrances thereon.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

Normally, indemnities are difficult to obtain as sellers oppose them and insist that the buyer should make its own judgement on risks based on due diligence. However, if specific risks have been identified during due diligence, those can be covered by indemnities, including with respect to intellectual property. Narrow indemnities against the results of ongoing litigation or ongoing tax audit are more likely to be agreed. Issues that are harder to track for the company, such as cybersecurity and data privacy, are more likely to be covered with representations and warranties than indemnities. Another reason for buyers not to press too hard for indemnities on privacy issues is that in Russia, the risks are effectively limited to regulatory and compliance, with fines much lower than those seen in the European Union. Any adverse impact of individuals' claims has been negligible so far, and class actions have been introduced only recently and are still rare in Russia.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

The IP representations given as true in all respects are rare. More often than not, there are materiality qualifiers and it is not uncommon for different categories of IP and technology matters to have different and specific materiality criteria or thresholds specified. The qualifiers may depend on a range of issues, including the territory and scope of the warranty. If, for instance, the territory for the representations and warranties is limited (eg, to Russia, or Russia and the Russian-language market in case of a Russian target), the buyer is more likely to lower materiality thresholds compared to matters beyond the principal market. Warranties relating to the rights provided by third parties tend to have higher materiality thresholds.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

Over the past couple of years the Russian market has seen an increase in technology-related deals, and the forecast is that the industry will become even more attractive for investment, considering projected state financing and overall prioritisation of the digitalisation of the Russian economy, which is the focus of one of the national strategy programmes. The main players on the market are large IT and telecom companies, which are seen to be developing their businesses to diversify and cover more areas and offer universal services to their clients. Other prominent deal makers include the state-controlled banks Sberbank, VTB and Gazprombank, and the Russian sovereign investment fund. The largest M&A deals in 2018 and 2019 were executed with respect to online applications, including taxi services, food delivery, online audio-visual services and online e-commerce retailing platforms. There is a lot of interest in blockchain-based technologies and services, especially in finance.

As part of the initiative to attract investment, Russia has approved the first reading of a bill on experimental legal regimes in the sphere of digital innovations, or innovation sandboxes. Some of the areas this initiative should accelerate are unmanned vehicles and blockchain projects in finance. The bill may become law by the end of the year.

Due to its engagement in most of the regulatory initiatives and projects related to new technology development, the Autonomous Non-Commercial Organisation Digital Economy is becoming consistently more important in that area. This non-governmental organisation has major IT companies, state banks and ministries among its founders and as members of its supervisory board.

While the digital economy market is developing rapidly, the law does not always manage to keep up. Despite active discussions and a number of regulatory developments concerning tokens, cryptocurrencies and online investments, Russia's existing legal system lacks a unified approach to regulating these technologies and their implementation. Starting from 1 October 2019, the provisions of the Civil Code of Russia came into force introducing a new form of rights – digital rights – and certain rules applicable to them. The new provisions are sometimes inconsistent (eg, digital rights are categorised as both property rights and contractual rights) and will remain nonviable until the adoption of the supporting system of ancillary laws and regulations. Such laws include the bill on digital assets (subject to the president's signature, likely to enter into effect on 1 January 2021) and Law 259-FZ of 2 August 2019 on, among other things, the attraction of investments through investment platforms, which came into force on 1 January 2020, but has not been widely implemented yet.

The bill on digital assets has been in preparation and discussions for around two years, and is still causing criticism from businesses, especially for its regulation of cryptocurrencies. The last version circulated in mid-May 2020 for public discussion received negative reactions from the authorities as well, specifically for the suggestion to make cryptocurrencies subject to arrest and seizure, while legal turnover is prohibited. If the current approach persists, the use of cryptocurrency in payments may become illegal in Russia.

Some of the other legislative initiatives in the sphere of technology may result in further limitations for the market. Thus, the State Duma (Russian parliament's lower chamber) adopted a bill in November 2019 (now signed into law) introducing a mandatory list of Russian software applications that will have to be pre-installed on smartphones, smart TVs and computer devices sold in the country, including those imported. This suggestion falls within the recent trend for supporting local software and hardware by Russian legislators and regulators, which is greatly criticised because, in many cases, there are no Russian alternatives to foreign programmes and equipment. Application of the requirement initially scheduled for 1 July 2020 was pushed to 1 January 2021 due to covid-19.

Another bill suggests introducing limits on foreign participation and control over 'significant' internet companies. The limitation is similar to the one already in place for mass media and telecom businesses. This initiative has already had a negative impact on the share prices of the largest Russian IT companies and is heavily criticised by the industry.

Coronavirus

21 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programs, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Despite the growth of traffic and demand for online services in general, the Russian telecom industry is expecting a substantial loss of profit in the first and second quarters of 2020 due to covid-19 negatively impacting annual results. In June 2020, three months into quarantine measures in Moscow and some other regions of the country being applied, President Putin declared certain plans to support IT-companies, including decreasing social security payments from current 14 per cent to 7.6 per cent and a substantial decrease of profits tax from 20 per cent down to 3 per cent. Both measures were suggested to be introduced for unlimited period of time. At the same time, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation suggested revoking VAT exemption for sales and licensing of software starting from 2021. According to the Ministry, Russian IT companies currently profiting from this exemption will receive state subsidies instead. According to the industry, the lack of this exemption will negate any advantages gained from the other support measures.

Currently, telecom and IT-companies may rely on the support provided by separate regions to support small and medium-sized businesses (SMEs). Thus, Moscow government provides subsidies for SMEs to compensate for up to 50 per cent of commissions charged by online platforms for placement of information on goods and services. Among non-monetary support measures are:

- automatic prolongation of licences (including telecom and broadcasting licences);
- grace periods under lease agreements; and
- a moratorium on inspections and bankruptcies.

State support was also provided to a number of companies that the Russian government commission considered were vital businesses for the country, including oil and gas companies and major IT and telecommunication companies, especially those that operate critical infrastructure. The process of selecting the companies to receive state support was not entirely transparent.

Quarantine and isolation measures applied during the pandemic forced a revision of some of the procedures and requirements for validating documents and deals. Thus, regulatory adjustments can be expected to facilitate the use of electronic signatures and electronic powers of attorney. A bill allowing the online sales of prescription drugs has been accelerated, despite being in discussions since 2017. Another bill was introduced to enable a simplified procedure to get permission to use biometric data to enter into telecommuication service contracts.

KING & SPALDING

Alla Y Naglis
anaglis@kslaw.com

Xenia A Melkova
xmelkova@kslaw.com

Tsvetnoy Bulvar, 2
Entrance B, 5th Floor
127051 Moscow
Russian Federation
Tel: +7 495 228 8500
www.kslaw.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-412-5