GIR KNOW-HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Russia

Xenia Melkova and Alla Naglis
King & Spalding (Moscow)

SEPTEMBER 2019

GIR INSIGHT

1 What laws and regulations in your jurisdiction regulate the collection and processing of personal data?

The legislation on personal data in Russia consists of the Federal Law No. 152-FZ 'On Personal Data', dated 27 July 2006 (as amended) (Personal Data Law), and regulatory acts adopted in pursuance of its provisions.

Most regulatory acts in the sphere of personal data regulation are adopted by the government, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, and the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Media (Roskomnadzor).

Certain rules applicable to processing of personal data of employees can be found in the Labour Code of Russia No. 197-FZ, dated 30 December 2001 (as amended).

2 What other laws and regulations may prevent data sharing in the context of an investigation?

Apart from personal data, other categories of information restricted for sharing under Russian laws include, among others, trade secret, state secret, professional secret (medical secret, bank secret, etc), private correspondence, the details of individuals' private lives and individuals' images in certain cases. Various requirements for protection and measures against unauthorised disclosure of such information are set forth in specific laws and regulations.

Most relevant laws expressly specify that governmental authorities can have access to any kind of information in connection with an ongoing investigation, or generally, upon a reasoned request (as is the case, for example, under the trade secret regulation and healthcare regulation). Some regulatory acts provide for more specific terms of access to certain types of information. For example, article 26 of the Federal Law No. 395-1 'On Banks and Banking Activity', dated 2 December 1990 (as amended) contains an exhaustive list of persons and authorities that can receive information constituting bank secret. Investigative bodies are expressly required to obtain court orders or approval from heads of investigative authorities, depending on the stage of the investigation, to obtain such information.

By way of a general comment, in Russia, the very term 'investigation' is considered as something reserved to the authority of state. The term is not even used when referring to private procedures, which are called audits, internal checks and so forth. Therefore, Russian legislation contains no specific provisions concerning private investigations, and access to personal and other data by legal entities as part of such investigation is in all cases subject to general rules. For example, labour laws specifically restrict certain categories of information that an employer is entitled to request and collect (thus, information on criminal record can be requested only for particular types of employment, eg, in the educational sphere, but not in any other cases). These rules apply generally but may have considerable effect in situations when a private investigation is carried out.

3 What can constitute personal data for the purposes of data protection laws?

The definition of personal data set forth in the Personal Data Law is very broad and includes any information relating to an identified or identifiable individual (data subject). As a result, in many cases the determination of what is or is not personal data in a specific situation remains at the discretion of the regulatory authorities who tend to apply the broadest possible interpretation and consider practically any type of information as personal data, including employment data, meta data and even big data. Unfortunately, the main authority in the sphere, Roskomnadzor, mostly expresses its approach in oral discussions or in specific decisions or responses addressed to particular personal data operators, leaving little official explanation for reference. Some issues can be cleared in online guidances published on the official website of the authority from time to time, but Roskomnadzor is not eager to set its position in stone, and its position is not always consistent either.

The approach to consider IP addresses, cookie files and other computer data as allowing personal identification of the user, hence personal data, was confirmed by courts in cases such as the Ruling of Supreme Court of Russia No. 82-AD16-1, dated 30 March 2016, or Ruling of the Ninth Appellate Court of Russia No. 09AP-17574/2016, dated 23 May 2016. However, as Russia is not a common law jurisdiction, these cases do not form binding precedents.

4 Does personal data protection relate only to natural persons or also legal persons?

The Personal Data Law applies to personal data defined as information pertaining to individuals. Company data is not treated the same way, and can be considered open data (with regard to entity registration records and public reports) or can be protected as trade secret (or other proprietary information, eg, databases or similar) in accordance with the applicable requirements.

5 To whom do data protection laws apply?

The Personal Data Law does not expressly distinguish between data controllers and data processors. According to Russian legislation, any entity processing personal data is considered a personal data operator. Slightly different requirements may apply if the entity proves that it processes data under a direct and documented order of the personal data operator, and thus acts as a third-party processor.

In practical terms, the Russian regulatory authority tends to consider any legal entity with at least one employee other than the general director (CEO) as personal data operator and expects it to comply with Personal Data Law requirements, including being entered as data operator in the state register (in the absence of applicable exemptions).

6 What acts or operations on personal data are regulated by data protection laws?

Pursuant to the Personal Data Law, processing means any action (process) or a combination of actions (processes) performed with or without the use of automated means, including collection, recording, systematisation, accumulation, storage, modification, extraction, exploitation, transfer (distribution, provision, granting access), anonymisation, blocking, deletion or destruction of personal data.

7 What are the principal obligations on data controllers to ensure the proper processing of personal data?

The principal obligation of all personal data operators is to ensure that the collection and processing are performed in accordance with the requirements of the Personal Data Law, ie, that data is collected on valid grounds (under consent, contract or other) and processed in accordance with lawful and valid purposes for which it was collected. This obligation always remains irrespective of whether other specific requirements (eg, those on data operator registration) apply to a particular data operator.

Operators are also required to ensure adequate and sufficient data protection measures, including legal, organisational and technical measures. Some measures are expressly named in the Personal Data Law, some are left at the operator's discretion. Separate regulations establish requirements for protection of different categories of information systems depending on the level of potential threats. Operators are required to have their IT systems audited with respect to the processing of personal data to determine which category and threat level they fall into and to implement the corresponding safety measures.

Another major requirement is to register with the state register operated by the competent supervisory authority (Roskomnadzor), which immediately puts relevant operators in the pool of monitored entities. There are certain exemptions from the obligation depending on the type of data processed; however, the operator generally exempt would still be required to get registered if any (even the smallest) piece of its data processing activity falls out of the list of exempt types.

Starting from 1 September 2015 Russian personal data regulation also contains a data localisation requirement. Under the provisions of article 18(5) of the Personal Data Law, data operators are required to procure for the recording, systematisation, accumulation, storage, modification and extraction of personal data pertaining to Russian citizens with the use of databases physically located in the territory of the Russian Federation. That requirement was initially designed to target major online services operating massive databases of personal identifiable information. However, the rule applies to any operator, including numerous companies storing their data in the clouds, if such clouds are located on servers outside the territory of Russia, or in corporate information systems located on servers of head offices outside Russia. Considering that the compliance with the data localisation requirement entails substantial changes in IT structure and significant money and time investment, a considerable number of players in the market decided to hold off from action until addressed directly by the regulatory authority. This approach may change shortly, as the Russian parliament is currently discussing a dramatic (200 times) increase in administrative fines for the failure to comply with data localisation requirements (more details in question 20).

Data extraction by third parties for data collection purposes

8 Before data extraction by third parties commences, should steps be taken to ascertain whether non-locally generated data was lawfully transferred to, or within, your jurisdiction in the first instance?

Russian personal data regulation makes no distinction between personal data of Russian citizens generated within or outside of the borders of the Russian Federation. The general rule is for any operator processing this data to do so in compliance with Russian laws.

There are no legal requirements to ascertain any issues prior to data extraction, unless specified in the data operator's internal personal data policies or procedures. Typically, confidentiality agreements and corporate data processing policies include the obligation of the entity to notify its contractual counterparties and individual data subjects of the facts of disclosure of their information to state authorities within a fixed period of time.

9 Are there additional requirements where third parties process the data on behalf of the entity to which data protection laws primarily apply?

As a general rule, third parties processing data on behalf of the original operator are responsible for compliance with the Personal Data Law and the terms of the mandate they have received from the data operator. In practice, the regulatory authority expects the mandate to be documented as a written agreement with clear and exhaustive terms and conditions of data transfer and processing, as well as requirements for its protection.

Pursuant to the provisions of the Personal Data Law, the original operator (data controller in terms of the EU regulation) remains responsible to personal data subjects, while the third-party processor is responsible to the operator.

10 Is the consent of the data subject mandatory for the processing of personal data as part of an investigation? And how can consent be given by a data subject?

In public investigations, Russian Criminal Procedure Code, the main piece of legislation regulating criminal investigation and proceedings, does not establish a requirement to obtain individuals' consents for processing of their personal data in the process of a criminal investigation. Federal Law No. 3-FZ 'On Police', dated 7 February 2011 (as amended) and Federal Law No. 144-FZ 'On Operational and Investigative Activity', dated 12 August 1995 (as amended) do not require a data subject's consent in investigation either. However, both laws specify that investigative authorities are not allowed to disclose information concerning the individual's private life, family or personal secrets, and reputation that become known to them in the course of investigation without the relevant individual's consent, unless the federal law expressly states otherwise. Federal Law 'On Police' expressly states that police authorities are entitled to process personal data of citizens without their consent.

Rather than consent, enforcement authorities in public investigations rely on other legal grounds for processing of personal data. Personal Data Law provides for a list of cases where the personal data can be processed without the consent of the data subject. Such grounds include, among others, processing for the purposes set in international treaties, processing in connection with the participation of the relevant subject in criminal, civil, constitutional or administrative proceedings, processing in the interest of protection of life, heath or other vital interests of the data subject, and processing of data required for the discharge of state authorities' functions. While this list does not expressly refer to investigative activities, it is widely presumed that police and enforcement authorities are entitled to obtain any information as per their request. The Personal Data Law does expressly allow investigative authorities to process even sensitive and biometric data without data subject's consent at various stages of investigation.

Some scholars express the opinion that enforcement authorities should obtain written consents prior to performing investigative actions that may reveal personal data and private information, as there is no clear exemption for investigative activities in the Personal Data Law. However, public investigations are not transparent enough for the monitoring of such cases, and there is no indication that the expressed approach is supported by the governmental authorities or courts.

In private (corporate) investigations, general rules of personal data processing apply to entities performing such investigations, including the requirements to obtain a data subject's consent or perform data processing on other legal grounds (for example, under a contract). In the absence of specific regulation of internal investigations, neither the employer, nor the employee has legal protection in case the procedure results in a labour conflict. Noteworthy is that the Russian Labour Code expressly states that employers are not allowed to transfer employees' personal data to third parties without their consent. While in practice, employees are rarely opposing companies in the course of internal investigations, the prudent approach would be to have a consent collected from every employee prior to commencement of the investigation by the employer.

11 If not mandatory, should consent still be considered when planning and carrying out an investigation?

In public investigations: provided an investigative action was carried out in accordance with relevant legal requirements, such as the requirements of the Criminal Procedure Code for criminal investigations, absence of consent for processing of personal data would not affect admissibility of results.

Under the Criminal Procedure Code evidence is considered inadmissible if obtained in breach of its requirements. And since an individual's consent is not explicitly required, its absence has not been viewed in criminal cases as effecting the quality of evidence.

In private investigations, as mentioned above in question 10, it is prudent for the employer to obtain preliminary consents for processing of employees' data in case of internal investigations. Consents to data sharing for potential investigations can be obtained at the start of the employment as part of the overall employment package. However, considering that Russian regulation requires data subjects' consents to be clear and specific, especially when it comes to transfer to third parties, such an approach is not entirely risk-free, and the maximum compliance effort would ideally require collecting consents for a particular investigation with indication of specific purposes and details of third parties (auditors, lawyers) to whom information will be transferred during such investigation.

12 Is it possible for data subjects to give their consent to such processing in advance?

As described in questions 10 and 11, it may be more practical for large corporations to obtain preliminary consents to all potential investigations (for example, at the conclusion of employment contract), given that it may not be feasible to collect all consents if and when needed to start the investigation (and bearing in mind that certain data subjects may intentionally withhold consents to impede the investigation process). While this approach is not risk-free, considering the overall requirement to specify exact purpose of processing and the transferees of data, which may not be possible in advance, there are no reported cases at the moment challenging it.

There is no official procedure for individuals to provide preliminary consents directly to state investigative authorities. However, as mentioned above, state authorities normally rely on other legal grounds for personal data processing, rather than data subjects' consents. For the transfer of personal data to state authorities by the employers, it is not uncommon for legal entities to include in their internal personal data policies provisions specifying that the company is entitled to provide state authorities with any information it processes upon request. Such provisions are also very common for confidentiality and non-disclosure agreements. By accepting relevant policies and signing confidentiality agreements, individuals and entities provide their consent to such disclosure of their information in advance.

13 What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

The Personal Data Law established the general right of the data subjects to have access to their data and information on its processing, to request modification, update or deletion of such information. All these rights should remain available to data subjects in the course of a private investigation.

For public investigations, the law expressly limits the above rights. The limitations can depend on the role of the individual in the investigation and its relevant procedural rights, such as rights to familiarise oneself with case materials. They can also be the result of the principle of non-disclosure of information on preliminary investigation set in the Criminal Procedure Code.

Rights to access case materials are also granted to participants in civil proceedings, as well as in administrative and arbitration proceedings.

Transfer for legal review and analysis

14 How are law firms, and legal process outsourcing firms, generally characterised in your jurisdiction?

Normally, any entity processing personal data is considered a personal data operator in the terms of the Russian legislation. A party may be considered as a third-party processor if there is documentary evidence of a mandate to process the data originating from the data operator and including terms and conditions of such processing. In any case, a third-party processor is obliged to comply with the same requirements of the law, with the exception of the fact that it is not required to obtain data subject's consent.

Law firms and other consultants normally work under relevant service contracts that contain terms of confidentiality of client information, including any personal data it may include. If a law firm or another consultant is specifically engaged to conduct a private investigation involving work with a bulk of personal data, it is advisable to have the client's instructions specifically address the personal data processing issues, including the obligation to ensure protection of data and its destruction or return upon the fulfillment of the assignment.

15 Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Operators of personal data are required to obtain a data subject's consent to transfer his or her data to a third party, unless such transfer is expressly allowed by law (for example, some state authorities automatically share information with other authorities). In practice, the regulatory authority requests such consents for transfer to be express and specific, naming precisely the third party that will receive the data, as well as the purposes of the transfer and scope of third-party processing.

It is worth mentioning that the regulator's approach is not entirely consistent with respect to the transfer of data without a clear mandate for third-party processing, for example, a transfer of data to an affiliate company under corporate procedures and policies. Recently, the competent authority has formed a tendency to conclude that the absence of a specific purpose of processing by the recipient set in a written contract between the two parties renders such data transfer unreasoned and invalid. Considering this, it is advisable to have a clear contractual arrangement in place with any third party to whom personal data is transferred setting forth the terms and purposes of data processing.

16 What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

The Personal Data Law does not prohibit transborder transfer of personal data, subject to certain requirements. Transborder transfer is simpler (and does not require the data subjects' written consent) if the data is transferred to countries that are parties to the 1981 Strasbourg Convention for the protection of individuals with regard to automatic processing of personal data or to jurisdictions that are viewed by Russia as providing adequate protection of personal data (the list of such countries is adopted by the Russian regulatory authority). In all other cases, a written consent of the data subject is required. Exemptions are set for transfers under international treaties, under federal laws, if required for national defence purposes or for safety of transport, under a signed contract to which data subject is a party, or for protection of life and health of data subject or third parties, if obtaining a written consent is impossible. Most importantly, pursuant to the above regulatory provisions, Russia does not consider the United States as a jurisdiction providing adequate protection of personal data. Thus, a transfer of personal data to third parties in the United States (or to servers located in its territory) requires the written consent of the data subjects.

Transfer to regulators or enforcement authorities

17 Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

Pursuant to the provisions of the Criminal Procedure Code of Russia, seizure of objects and documents containing any state or other type of legally protected secret (that would arguably include the personal data, although it is not expressly mentioned) is performed by enforcement authorities only upon a court order. The same applies to seizure of information on deposits and bank accounts of citizens, correspondence, information on calls and messages, recording of calls. The general principle, specified in the Federal Law No. 144-FZ On Operational and Investigative Activities, dated 12 August 1995 (as amended), states that any investigative activities restricting constitutional rights to the secrecy of correspondence, telephone conversations, mail and other communications, as well as inviolability of residence, require a court decision.

In addition to the above, investigative authorities also have rights to request provision of certain personal information in accordance with the provisions of regulation in the sphere of telecom and communications. In force since 1 July 2018, the rules of the 'Yarovaya Law' (labelled under one of its authors) require telecom operators to store and provide at request of investigative authorities the records of all voice data, correspondence, pictures, videos and other messages exchanged, downloaded, shared or uploaded by users, as well as metadata on the fact of receipt or transmission of information. The correspondence is to be stored for six months from the moment of transmission, and the metadata on communication for three years. Authorities are also entitled to request decryption keys if the above data was encrypted. Similar requirements are set for the information distribution administrators (ie, persons operating information systems and applications designed or used for receipt, transmission, delivery or processing of electronic messages of online users), including operators of online messaging systems. These parties are required to store text messages, voice information, images and other electronic messages within six months of transmission and relevant metadata and information on users within one year of transmission. Operators are required to provide stored information to investigative authorities and state security services upon request.

Transfer of personal data to enforcement authorities as part of reporting potential crime should (even if not specifically listed) also be viewed as exempt from the requirement to obtain a data subject's consent, as other grounds for processing can be considered applicable (see question 10).

18 Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

Transfer of personal data to other jurisdictions is regulated by general provisions of the Personal Data Law on transborder transfer (as described above in question 16). According to the provisions of the Personal Dara Law, transborder transfer to a jurisdiction that is not viewed as providing adequate protection of personal data is possible in certain cases, including on the basis of the data subject's written consent or in situations specified in Russia's international treaties. For example, one of these treaties is the Convention on legal assistance and relations in connection with civil, family and criminal cases signed in Minsk in 1995 by the members of the Commonwealth of Independent States (CIS). Russia is a party to more than 50 bilateral treaties on legal assistance with various countries.

19 What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

When receiving a request for disclosure of data from regulatory authorities, personal data operator should review its internal documents and commitments to ensure compliance with any obligations to data subjects and third parties. It is also advisable to look into the scope of the request for consistency with the statutory requirements, as sometimes the requests may be too broad.

Considering legal rights of data subjects to be informed of processing of their data, it may be advisable to inform them of disclosure of their information to state authorities (while the operator is not obliged by law to do that unless requested by the data subject), provided that in some cases a subject's rights to such information may be restricted (as mentioned above), for example, in the case of an ongoing investigation with respect to such data subject. Other restrictions may also apply. For example, Federal Law No. 40-FZ 'On Federal Security Service', dated 3 April 1995 (as amended), requires that persons cooperating with the authority do not disclose any information they became aware of during such cooperation. The Federal Security Service may be one of the authorities requesting disclosure of data as part of a state investigation or under the provisions of telecoms regulation.

20 What are the sanctions and penalties for non-compliance with data protection laws?

Various violations of the requirements of the Personal Data Law are punished under the Russian Code of Administrative Offence (article 13.11) with different sanctions, including, mostly, administrative fines up to 75,000 roubles. For example, the maximum amount of fine is applicable to cases of transfer of personal data to third parties without obtaining data subject's written consent. Transferring data to regulators and enforcement authorities is extremely unlikely to be considered as a violation of the data protection regulation. The Russian State Duma is currently discussing amendments to the regulation to introduce administrative sanctions for failure to comply with requirements for personal data localisation in the territory of Russia with fines up to 18 million roubles.

Specific sanctions are set for failure to comply with legal requirements of investigative authorities, which may include failure to provide information upon request. The maximum sanctions under relevant article 17.7 of the Code of Administrative Offence for legal entities amount to 100,000 rouble fine or suspension of activities for up to 90 days. Criminal responsibility may also apply if relevant actions qualify as obstruction of justice. Criminal penalties under Russian Criminal Code apply to individuals only.

Continuing obligations on original and intervening data controllers

21 What are the continuing obligations on the original data controller that apply in an investigation?

Personal data operators are required to comply with the provisions of the Personal Data Law, irrespective of whether there is an investigation under way. The only specific provisions of the Personal Data Law that may apply in the course of a public investigation is the restriction of a data subject's rights with respect to information on processing of his or her personal data.

22 What are the continuing obligations on any intervening data controller that apply in an investigation?

As mentioned in question 5, Russian legislation does not distinguish between data controllers and data processors. Thus, any intervening data operator (or a third party processing data on the basis of the mandate from the original operator) is subject to compliance with the same requirements set in the Personal Data Law for the original operator of data. Third-party processors are also required to ensure processing of data in accordance with the terms and conditions of relevant agreement entered into with the original operator for processing of personal data. It is important for third-party processors to bear in mind the time frame for data processing in accordance with the original operator's instructions and ensure destruction of personal data transferred to them upon fulfillment of the purposes of the relevant mandate.

Relevant materials

23 Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

These are:

- Federal Law No. 152-FZ 'On Personal Data', dated 27 July 2006 (as amended);
- Criminal Procedure Code of the Russian Federation No. 174-FZ, dated 18 December 2001 (as amended);
- Federal Law No. 3-FZ 'On Police', dated 7 February 2011 (as amended);
- Code of Administrative Offences of the Russian Federation, No. 195-FZ, dated 30 December 2001 (as amended);
- Federal Law No. 144-FZ 'On Operational and Investigative Activities', dated 12 August 1995 (as amended);
- Federal Law No. 149-FZ 'On Information, Information Technologies and Protection of Information', dated 27 July 2006 (as amended); and
- Federal Law No. 126-FZ 'On Telecommunications', dated 7 July 2003 (as amended).

Xenia Melkova

King & Spalding (Moscow)

Xenia Melkova's principal areas of practice are data protection issues and regulation of information distribution, corporate and regulatory matters within the TMT sector, advising clients on employment issues, business structuring, content production, software development and licensing. A senior attorney with Moscow office, Xenia has extensive experience in advising clients in different industries on the issues of the personal data protection regulation and various compliance strategies. She also specialises in regulation of new technologies and IP matters, focusing on the film production and distribution industry, software/hardware development and licensing matters, and advises foreign television channels on regulatory issues relating to their broadcasting activity and carriage deals in Russia.

Alla Naglis

King & Spalding (Moscow)

Alla Naglis is a partner and leads the TMT and IP practices in King & Spalding's Moscow office. She has over 20 years of advising on a daily basis major US, European and Russian companies on virtually all aspects of media and entertainment industry (including, above all, film and television industry and matters related to cross-border production and financing, distribution and broadcasting issues), e-commerce and IT (including protection and enforcement of copyright and related rights on the internet), technology and know-how protection, plus licensing and domain name protection; and data privacy and security issues. The scope of her expertise ranges from counselling and contractual matters to regulatory advice and representation of clients in courts and arbitration. In the data privacy area, her experience includes counseling on internal compliance policies and audits for major international players, as well as compliance checks of local vendors or partners. Ms Naglis has been consistently ranked as one of the leading Russian TMT lawyers.

King & Spalding

King & Spalding is a full-service Global 50 law firm with more than 1,000 partners and associates in 20 offices across the United States, Europe, Asia and the Middle East. Founded in 1885, the firm is consistently recognised for the results it obtains, its uncompromising commitment to quality and its dedication to understanding the business and culture of its clients. The American Lawyer has ranked King & Spalding among the top 50 law firms in the world since 2005 and among the top 50 law firms in the United States since 1990 based on size.

King & Spalding's data, privacy and security practice regularly advises clients regarding statutory and regulatory requirements businesses face when handling personal and other sensitive information concerning individuals such as employees, consumers, customers or patients, in the US and globally.

King & Spalding provides substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy and public policy.

King & Spalding also has a destination TMT practice, with a client list that includes the biggest names in the global market. Our team has extensive experience counselling its TMT clients on complex, market-shaping issues, be it in the technology (including, software and hardware development and licensing and work on online activities) or media industries (such as the restructuring of TV channels operations in Russia).

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

www.kslaw.com

Xenia Melkova
xmelkova@kslaw.com

Alla Naglis
anaglis@kslaw.com