Baker McKenzie.

RUSSIA: CHECKLIST FOR COMPLIANCE INVESTIGATIONS

Investigations in Russia can present a variety of risks, ranging from violations of data privacy and employment law to criminal liability for disclosure of state secrets. This article provides a guide on what to do and not to do when conducting investigations in Russia.

OVERVIEW OF AREAS TO CONSIDER

Protection of personal data

Russian personal data law defines personal data broadly as "any information directly or indirectly concerning an identified or identifiable natural person (personal data subject)." Collecting, recording, systematizing, accumulating, storing, updating and similar acts require the consent of the data subject. However, there are certain exceptions to the consent requirement including:

- processing for employment purposes;
- processing *"for purposes established by an international treaty of the Russian Federation or by a law, or if such processing is necessary in order to allow the operator to satisfy duties, rights and obligations imposed by the law"*;
- processing necessary to protect the rights and interests of the operator or third persons or necessary to achieve a public purpose, provided that such processing does not breach the data subject's rights.

These exceptions have not yet been tested with Russian regulators or in Russian courts. Therefore, it is not clear how broadly they may apply.

The personal data law contains no exception or any special provision for the intergroup transfer of employee data. Thus, a company wishing to disclose employee personal data to another group company, such as a domestic or foreign parent company, is required to comply with the same statutory provisions that would apply to any third party disclosure. In other words, it must either obtain the employee's consent or rely upon a statutory exception.

Penalties for Violations

Failure to comply with the requirements of the personal data law during an investigation may lead to various negative consequences, including administrative liability and civil penalty for the company and criminal liability for individuals. Individuals involved in internal investigations could also be convicted for violating Russian data privacy laws under Article 137 of the Criminal Code (Violation of private life)[1] and Article 138 (Violation of communication secrets)[2].

These crimes may result in incarceration of up to 5 years. To the best of our knowledge, they have never been applied against individuals conducting internal investigations, however their broad wording suggests

[1] The article prohibits *"illegal collection or dissemination of information about private life of a person, which (information) is subject of personal or family secret, without this person's consent, or dissemination of this information in a public speech, publicly demonstrated works, or in the mass media"*. It also prohibits illegal public dissemination of information identifying crime victims under the age of 16 or details of their physical or moral suffering.

[2] The article prohibits *"violation of secrets contained in correspondence, phone communications, post, telegraph and other messages of citizens"*.

that such risks exist. In particular, in theory the mere reading of an individual's correspondence without consent could be considered a crime.

The recent position of the Constitutional Court, described in its Resolution 25-P, in our opinion, helpfully clarified how the risks of criminal liability under the aforementioned Articles could be mitigated. Resolution 25-P dealt with termination of an employee for sending commercial secrets information[3] to his personal mailbox. Among other things, the Court confirmed with the reference to ECHR practice, that the employer' surveillance measures do not violate employees' privacy, where the employees have no reasonable expectations of such (e.g. where the employees use corporate devices or mailbox for personal communications, knowing about potential or ongoing surveillance). Therefore, proper and timely notification of employees about surveillance measures should effectively decrease the risk of criminal liability for violation of Russian data privacy laws.

Administrative fines may be imposed, inter alia, for failure to obtain a data subject's consent to data processing/ transfer, and (less likely to apply to foreign employees conducting an investigation) also for failure to publish a privacy policy (i.e., a notice to all employees whose data will be collected explaining the rules and procedures of collection) on a website collecting personal data, failure to appoint a data protection officer (or responsible organization), and failure to take necessary organizational or technical security measures. Administrative liability may be imposed on (i) a non-compliant legal entity and/or (ii) its responsible directors or officers.

Civil penalties may include damages for "moral harm" (a Russian legal concept roughly equivalent to "pain and suffering" in the US) and/or a court order to cease violations.[4] Administrative penalties may include an administrative fine, the maximum amount of which is currently approximately 1,200 USD.[5]

In addition, a prohibition on entering Russia may be issued against a foreigner (e.g. a foreign citizen holding a senior managerial position in a company) based on two or more administrative violations within three years. This rule applies to any administrative violation imposed by any competent authority authorized to hear administrative cases (i.e., courts of law, judges and authorized regulatory and law enforcement agencies). For instance, a single fine for violation of a speed limit, plus a fine for violation of personal data laws may be sufficient. A foreign citizen subject to such a prohibition can be stopped at the Russian border and denied entry even if he/she has a valid Russian visa.

Violation of an employee's data privacy rights can also make it difficult to discipline or terminate the employee as he/she may use the violation to challenge the legality of any remedial action.

State secrets and other information sensitive for security of the Russian Federation

Some Russian custodians could be in possession of what is called a "state secret" or of other information which Russian law-enforcement authorities may consider as being important for Russian national security. Disclosure of this information during an investigative interview or otherwise during an investigation could

[3] The concept of "commercial secret" in Russian law is aimed at protecting trade secrets and other confidential and commercially sensitive information.
[4] Personal Data Law, Article 24.2
[5] COA, Article 13.11

lead to criminal prosecution of both custodians (under Criminal Code's Article 275 "Treason"[6] or Article 283 "Disclosure of State Secrets"[7]) and investigators (under Article 276 "Espionage")[8].

The likelihood of an investigation or prosecution in such a case depends on a number of factors including (1) the degree of access to state secrets or other sensitive information held by the subject and the subject's employer, (2) whether participation in the interview is consistent with the terms of that access, (3) the subject matter of the interview and (4) whether the Russian government has an independent reason for wanting to investigate either the subject or the subject's employer.

Attorney-client privilege

Russian law establishes a concept of attorney-client privilege very similar to other civil law countries. This concept is called advocate's secret (advokatskaya taina) and protects relations between the client and "advocates" (attorneys licensed to represent defendants in criminal proceedings). While this privilege formally exists, in practice it can be overcome if the advocate is criminally charged.[9] Some cases were also publicly reported where law enforcement authorities disregarded the effective privilege and seized the relevant data in order to put pressure on the advocate and his / her client.

Despite the limitations of the privilege under Russian law, correspondence with Russian external counsel should still be marked as privileged in order to protect the privilege in U.S. proceedings.

Employment law considerations

Russian employment law is very formal and protective of employees (a legacy of Russia's socialist history). As a result, it is normally very difficult to terminate an employee, even if the company knows about his / her wrongdoing. In most cases, it is only possible to terminate an employee after two disciplinary actions in one year.

In addition, a disciplinary sanction must be imposed within 1 month of the day on which the breach of discipline was discovered - i.e., when an employee's supervisor became aware of the violation. "Supervisor" in this sense is defined as a person to whom an employee reports (i.e., an immediate manager or general manager of the employer or any other relevant manager).

Furthermore, Russian employees are not obliged to retain data relevant to an investigation unless expressly instructed so by their formal chief. Such an instruction should take form of an order of the general director or another senior manager of the Russian legal entity empowered to issues such orders. If the order initiates an internal investigation (an audit or a review), it can also extend the limitation period for imposing a disciplinary measure from 6 months (from the date the wrongdoing was committed) to 2 years.

[6] Punishable with up to 20 years of imprisonment with or without a fine, the amount of which could significantly vary.
[7] Punishable with up to 4 years of imprisonment with or without a prohibition to conduct certain activities for up to three years.
[8] Punishable with up to 20 years of imprisonment.
[9] With prior commencement of criminal proceedings personally against the advocate or with recognizing the advocate as indicted person within the ongoing criminal proceedings.

Russian employees quite often challenge terminations with the labor inspection[10] and/or in court to restore their employment. If there has been a procedural violation in their termination, they have good chances of success, which increases the risks of such a challenge and attendant negative publicity for the company.

DO'S AND DON'TS

Do:

- Before taking any action, consult with qualified Russian counsel with expertise in labor and data privacy law;
- Develop a thorough compliance program prohibiting conflicts of interest, improper remuneration on the company's behalf, establishing line of reporting about compliance violations, collect personal data consents, notify employees what could happen with the their data if obtained by the company in an internal investigation;
- Obtain full and valid personal data consents before collecting employee data, if no consents were obtained earlier or these earlier consents are not adapted to the purposes of the internal investigation;
- Issue an order officially initiating an internal investigation before interviewing employees or collecting their data;
- Mark your correspondence with Russian external counsel as legally privileged and confidential.
- Keep in mind that communications with company forensic investigators may not be covered by attorney-client privilege.
- Before each interview verify whether the custodian legal possession of any information considered to be state secrets and whether the proposed interview is consistent with the terms and conditions of such access;
- If the investigation is conducted with an eye towards possible prosecution or disclosure outside of Russia, follow applicable foreign rules for conducting interviews, such as, in the case of matters in the U.S., giving Upjohn warnings;

Don't:

- Collect, review and send abroad personal data without express consent of the relevant employee;
- Assume that communications with outside counsel will be considered privileged by the Russian law-enforcement authorities;
- Push subjects to provide information claimed to be a state secret or sensitive to security of the Russian Federation without prior seeking legal advice;

[10] A "labor inspection" is a state authority charged with overseeing employers' compliance with the requirements of Russian labor law. Labor inspections can issue orders to restore the employment of a terminated individual and other binding orders related to labor law issues.

- Terminate the wrongdoer without making sure all requirements of Russian labor law have been satisfied.

FREQUENTLY ASKED QUESTIONS

1. Do Russian data privacy laws apply to transfers of Russian citizens' data outside of Russia?

Yes. In many cases, they require obtaining express written consents for cross-border transfer of such data.

2. Is taking notes during interviews considered processing of personal data?

Possibly. Given the breadth of the law, notes typed electronically could be considered processing of personal data. Handwritten notes are less likely to be recognized as such.

3. How aggressively are Russian data privacy laws enforced?

Not aggressively, but the laws are written broadly and the government could decide to start enforcing them aggressively at any time.

4. Who is most at risk for violations of Russian data privacy laws?

Russian legal entities, their general managers and employees responsible for data protection. Foreigners, including company employees and outside lawyers, accountants and investigators can also be held liable if they suborn a violation.

5. Does Russia have a system of self-disclosure?

Russia has a system of self-disclosure rule in bribery cases. Self-disclosure in bribery cases may provide certain benefits for indicted persons (including potential release from liability). These rules have been applied for approximately one year in criminal corruption cases against individuals. Similar rules for legal entities were introduced in August 2018, but their application is still unclear.

6. Are companies required to self-disclose violations?

No. Only individuals are required to report about certain type of crimes related to significant public exposure, such as terrorist attacks. There is no requirement to report about bribery, fraud and other white-collar crimes.

7. Does Russia have an extradition treaty with the United States?

No.

8. Does Russian law prohibit foreign bribery?

Yes, it provides criminal penalties (in the case of individuals) and administrative penalties (in the case of legal entities and individuals).

9. What is required for terminating an employee for acts of fraud or corruption?

Termination of an employee without a criminal conviction is extremely difficult. Therefore, in most cases, companies usually negotiate a severance package. The amount of the severance payment is dependent on the case, but in our experience is usually equivalent to 3-6 months salary.

10. Does Russian law impose any special requirements on the conduct of interviews (i.e. required presence of a works council representative)?

No.