CROSS-SECTORAL COMMITTEES

COMPLIANCE & ETHICS COMMITTEE

CHAIRPERSON:

SVETLANA MAKAROVA,
NOKIA

DEPUTY CHAIRMAN:

ALEXEY KHAKHULIN,
PJSC FORTUM

APPLICATION OF NEW COMPLIANCE TECHNOLOGIES IN A DYNAMICALLY CHANGING WORLD

ISSUE

The outbreak of the COVID-19 pandemic has forced companies to reconsider their priorities in many areas. It has obviously led to severe financial problems for both companies and workers in all industries. Since businesses are currently resuming their activities while adjusting to the twists and turns in the "new normal", many compliance challenges remain, and new compliance challenges will arise as well, requiring proper handling.

RECOMMENDATIONS

- Companies need to be flexible, adapt to rapid changes in their industries and the market in general, and revise their strategic goals where necessary, with a commitment to ethical and compliance principles.

- Companies need to pay attention to the value of an informed compliance culture and foster a culture of ethical behavior and business ethics to avoid exacerbating the negative financial impact of the crisis. The current situation is already complex enough and does not need to be further complicated by the legal consequences of violations in the field of compliance, including criminal ones.

ISSUE

- The number of legal requirements is continuously growing. Amid such regulatory pressure, compliance experts are faced with a host of new tasks requiring immediate attention. How can we maintain the golden standard of compliance in a fast-changing regulatory environment?

RECOMMENDATIONS

- Compliance is becoming an integral element of corporate culture and helps build business based on high corporate standards. Corporate culture has a defining value for companies. Building a corporate culture is the CEO's responsibility, but it requires input from each and every employee. Understanding corporate values is crucial for creating a trust-based business environment. Today the presence of policies and procedures alone is not enough. It is essential to seamlessly incorporate these procedures into a company's activities or, in other words, create a balance between adequate control and acceptable risks.

ISSUE

- The rapid growth of technology cannot be stopped. The use of AI, process automation, and more is turning technological processes into a driver of change, with even more new compliance challenges emerging along the way. Compliance departments operate using modern automated systems. Such systems are often not interconnected and are not flexible in relation to regulatory changes, which requires significant costs for their modernization.

RECOMMENDATIONS

- The strategy pursued by a company determines the use of technology across the company and in all areas of its activities. Reasonable use of technology is another factor that is no less important. The company's maturity and the availability of methods and internal processes as well as the preparedness of its personnel for automation are factors to be taken into account. Sensible use of new technology helps companies progress in all their areas.

PROCESSING OF EMPLOYEES' PERSONAL DATA IN THE CLIMATE OF THE COVID-19 PANDEMIC

The COVID-19 epidemic has forced many companies to switch a significant number of their employees to remote working, which has entailed additional difficulties in terms of processing personal data and has negatively affected the employers' ability to monitor the actions of their employees.

ISSUE

Remote work requires the processing of personal data using employees' devices and using corporate devices located away from the employer's premises. This issue is not new per se, but it is obviously the first time the Russian economy has faced personal data processing at such a large scale.

RECOMMENDATIONS

In this regard, the following activities are of particular relevance:

- revising the processes of personal data processing and changing previously developed lists and methods of personal data processing;
- adjusting employers' corporate regulations in line with changes in the characteristics of personal data information systems;
- making sure data contained in personal data controllers' registers are up to date and updating such data in a timely manner;
- ensuring the confidentiality of personal data using technical means.

In cooperation with personal data operators, the public authorities concerned should collect and summarize data regarding the best practices of risk management with regard to processing the personal data of remote employees, as well as employees processing personal data collected by their employer using their personal devices.

ISSUE

Monitoring employees' activities becomes more difficult with an increase in the number of devices and processes to be monitored. For the purpose of monitoring employees' actions using technical means, an employer generally relies on the consent of the data subjects, which consent may be withdrawn. The withdrawal of consent to personal data processing may make such processing impossible and is extremely likely to be used by mala fide employees to protect themselves in the event of an investigation.

RECOMMENDATIONS

- Employers should assess whether their employment contracts and corporate regulations are relevant in terms of establishing a clear list of cases in which it is permissible to monitor employees' actions. Employers should analyze the legal grounds for such monitoring and develop a legal stance regarding additional grounds for processing personal data in the event of the withdrawal of consent thereto.

ISSUE

In certain constituent entities of the Russian Federation, the challenges arising from the pandemic have forced authorities to require employers conducting activities in certain industries to ensure mandatory vaccination of at least 60% of their employees. For example, in Moscow, employers have been obliged to submit employee vaccination reports electronically. Moscow employers were to upload these to the official website of the Mayor and Government of Moscow from July 1, 2021, to July 15, 2021. In many other regions, similar responsibilities have been introduced within different terms, etc. Employers have been obliged to submit the following information regarding their vaccinated employees: Individual insurance account numbers (SNILS), compulsory medical insurance policy numbers, series, and the number of identity documents or patents (for foreign citizens), as well as mobile phone numbers.

However, data on vaccination/non-vaccination are personal data and thus may not be disseminated without the respective employee's consent. At the same time, on its official website, the Federal Service for Labour and Employment (Rostrud) has explained that in Moscow Region, no consent is required to transfer employees' COVID-19 vaccination data to authorities, as such information is required for the purpose of preventing a threat to the employees' health and lives.

Considering the fact that the explanations above are not regulations and contradict each other, there exists a risk of claims against employers due to the unlawful transfer of employees' data to third parties.

RECOMMENDATIONS

- The employers carrying out their activities in the fields falling under regional requirements for ensuring vaccination of a specific number of employees should obtain their employees' consent to transfer of such employees' personal data to public authorities, for the avoidance of the risk of claims by the employees. Such consent shall include references to the respective documents issued by governmental sanitary inspectors and the authorities of constituent entities of the Russian Federation.

›› **More information on the Committee page**