ALRUD

# Newsletter

## *COVID-19: Key data protection and cybersecurity issues triggered by the spread of coronavirus infection*

April 13, 2020

### Dear Ladies and Gentlemen,

Spread of coronavirus infection made companies to change their daily practices in order to ensure continuous business operation without compromising individuals' safety.

In this newsletter, we elaborate on the most sensitive legal issues in terms of data protection, privacy and cybersecurity.

### Employers shall collect new categories of data about their employees

Among primary measures introduced due to COVID-19, companies were obliged to arrange employees' body temperature measurements and thereby carry out the epidemiological control on a company level. Moreover, some companies went further and started measuring the body temperature of individuals visiting their premises.

Shortly after, Moscow Mayor introduced a mandatory self-isolation for the individuals over 65 years and the ones having certain diseases, which also triggered the need to collect new categories of employees' health personal data and define additional purposes of their processing.

In light of this, the Russian data protection authority ("**Roskomnadzor**") issued its recommendations with regard to some COVID-related data protection compliance issues.

Further to Roskomnadzor's recommendations, we would like to outline some basic aspects that are important from the data protection perspective:

- There must be a legal ground for the data processing: Roskomnadzor confirmed that body temperature measurements constitute sensitive data, which means that applicable legal grounds are quite narrow. Russian employment laws lay down that employees' health data may be processed to an extent necessary to consider employee's capacity to perform his employment duties – as explained by Roskomnadzor, this may be used to justify processing of employees' personal data.

  As for the visitors' body temperature measurement, it is quite onerous to justify their health data processing in the absence of consent. Roskomnadzor advised that such individuals provide their consents by affirmative actions. However, we also believe that it may be an option to avoid keeping records of visitors' temperature and thereby avoid personal data protection concerns.
- Individuals shall be notified of data processing: Personal data processing should be transparent to all individuals concerned. This should be done via public notices placed in the company's premises and implementation/update of local data protection/privacy policies.
- The data shall be deleted on a timely manner: The data shall be processed no longer than necessary to fulfill the processing purpose declared – simply speaking, it means that the data shall be deleted, once processing purpose is fulfilled. In light of this, Roskomnadzor recommends that body temperature measurements are to be deleted within a day after they are collected.
- The data shall be kept secure and confidential: Processing of health data is a sensitive issue in terms of compliance and individuals' privacy – it is necessary to implement necessary security

Skakovaya str., 17, bld. 2, 6th fl., Moscow, Russia, 125040
T: +7 495 234 96 92, E: info@alrud.com
alrud.com

safeguards to preserve such data from unauthorized access, modification and other unlawful operations.

In this regard Russian laws set out specific requirements on processing and protection of personal data on hard copies (manually) – these requirements shall be kept in mind and properly implemented in case of keeping body temperature records.

## Employers are forced to transfer employees to remote work

Due to the current epidemiological situation and related legal developments, many companies do their business remotely – their employees work from home.

This triggers additional issues associated with the need to carry out control of employees' remote performance and ensure higher level of cybersecurity in order to preserve confidential information (personal data, trade secrets) from being compromised.

In light of this, companies should review their existing cybersecurity practices, such as the rules of the corporate assets use and carrying out technical monitoring of such use, monitoring employees email communications, etc.

We would like to draw your attention that current epidemiological situation does not imply any exceptions in terms of compliance with the Russian data protection requirements – it means that all companies' practices, including the ones mentioned above, shall be legally compliant, i.e., all policies/notices shall be properly implemented and communicated to employees, there must appropriate legal grounds for the data processing, etc.

## Position of European Data Protection Board

European Data Protection Board ("**EDPB**") published a statement on the processing of personal data in the context of the COVID-19 outbreak. Within the statement, the EDPB stresses that processing of personal data in the context of the epidemics shall be lawful, however it also refers to the legal grounds rather than consent, such as processing for the reasons of public interest in the area of public health, protection of vital interests or compliance with a legal obligation. In addition, the EDPB gives certain guidance on processing of electronic communication data, which is subject to additional legal requirements.

We believe that in certain cases both EU-wide and country-specific recommendations shall be taken into account by companies doing business in Russia – this may be relevant, for example, for the Russian companies of international corporate groups subject to GDPR.

## Protection of Company commercial information

Companies shall pay high attention to protection of their commercial secrets and confidential information during forced digitization of all processes. In order to increase the protective measures we recommend companies to introduce regime of commercial secrecy and the respective policies on how to deal with the company information assets. Introducing of this regime requires taking appropriate organizational, legal and technical measures.

Employers of developers and other employees involved in creation of IP should ensure proper formalization of such employees' job duties in the employment contracts and job descriptions in order to cover all IP objects created during remote work by the regime of so-called "work for hire" that evidences the employers' rights to these objects. With this, employers shall ensure proper transfer of the rights to IP objects from employees.

## Expected developments

Currently, a number of additional initiatives that entail data protection and cybersecurity concerns are being discussed. The most sensitive one relates to implementation of a self-isolation control system, which will likely involve quite extensive processing of citizens' personal data. However, it is not that clear how this system will be regulated and practically implemented.

*Please keep yourselves safe! We will be working for you and keep you posted on the relevant legal developments.*

Skakovaya str., 17, bld. 2, 6th fl., Moscow, Russia, 125040
T: +7 495 234 96 92, E: info@alrud.com
alrud.com

For up-to-date legislative news and business-related guidance in connection with COVID-19, please visit our dedicated webpage

COVID-19: What you need to know

We hope that the information provided herein will be useful for you. If any of your colleagues would also like to receive our newsletters, please send them the link to complete a Subscription Form. If you would like to learn more about our Data Protection and Cybersecurity Practice, please let us know in reply to this email. We will be glad to provide you with our materials.

*Note: Please be aware that all information provided in this letter was taken from open sources. Neither ALRUD Law Firm, nor the author of this letter, bear any liability for consequences of any decisions made in reliance upon this information.*

If you have any questions, please, do not hesitate to contact ALRUD partner


Maria Ostashenko

Partner
Commercial, Intellectual Property, Data Protection and Cybersecurity

E: mostashenko@alrud.com


Sincerely,
ALRUD Law Firm