Eurasia beyond Covid-19: Data protection challenges

October 15, 2020

alrud.com

COBALT | ALRUD | AEQUITAS LAW FIRM | VASIL KISIL

Russia:
Legal requirements for health data processing in context of new epidemiological requirements

ALRUD

New data processing activities carried out by employers in Moscow

Measurement of employees' temperature each 4 hours

Coronavirus tests for not less than 10% of employees shall be done each 15 days

Collection of employees' blood samples for the laboratory study by way of enzyme-linked immunosorbent assay (ELISA) on a coronavirus infection and related immunity to it

Collection of extended scope of employees' health data (chronical diseases, specified in the list of diseases adopted by Moscow City Health Department, pregnancy and etc.)

Decree of the Mayor of Moscow dated March 5, 2020 No. 12-YM (as amended on October, 6, 2020) "On the introduction of a high alert regime"; Decree of the Mayor of Moscow dated June 8, 2020 No. 68-YM (as amended on October, 6, 2020) "On the stages of lifting the restrictions established in connection with the introduction of a high alert regime"

New Moscow Mayor's Decree provides for more obligations

Starting from 12 October, 2020 Moscow employers must upload weekly, on Mondays, the following information about the employees transferred to remote work to the website of the Mayor and the Government of Moscow:

- Mobile phone number
- State registration number of the vehicle (if any)
- Numbers of electronic transport cards (if any)

- Is this requirement legal?
- Are employers obliged to collect these data from the employees?
- What if an employee disagrees?

Decree of the Mayor of Moscow dated October 6, 2020 No. 97-УМ

Kazakhstan:
Reformation of the Kazakhstan legislation and its impact on personal data processing

AEQUITAS
LAW FIRM

New Health Code and amendments to the Personal Data Law

- Establishment of an authorized agency in the sphere of personal data protection
- Setting out the personal data collection and processing conditions in a detailed manner
- Introduction of voluntary cyber insurance and the concept of "service ensuring safety of personal data"
- Establishment of additional obligations of an owner and/or operator, person responsible for the organization of the personal data processing
- Establishment of the procedure for the collection, processing, protection of personal medical data under the new Health Code

Ukraine:
Legal requirements for health data processing in context of new epidemiological requirements

VASIL KISIL

COVID-19 recommendations for employers

From June 22, 2020, Kyiv City State Administration encourages employers to systematically test their employees to detect new COVID-19 cases and prevent local transmission of the disease

The Ministry of Health recommends:

- transfer employees to remote work, if possible
- if not, ensure that the employees in the office keep distance
- periodically disinfect all surfaces and objects in use
- ensure flexibility of leave policies
- send the employees home immediately and notify their family doctor if they show any symptoms of acute respiratory illness

Minutes of the Meeting of the Emergency Response Headquarters dated June 22, 2020, No. 45; Recommendations for enterprises and employers to prevent the spread of acute respiratory disease COVID-19 caused by the SARS-CoV-2 coronavirus, developed by the Ministry of Health of Ukraine

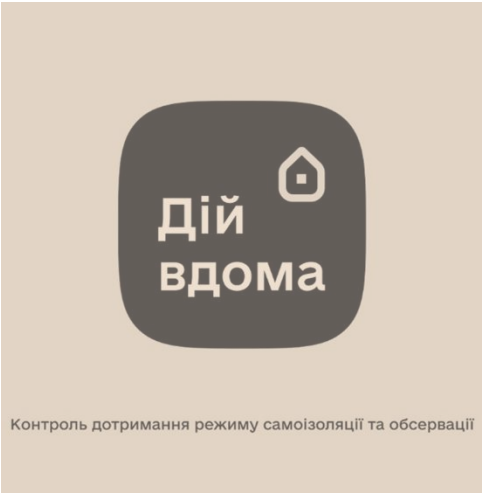
“Diy Vdoma” mobile app

This app was designed by the state to control 14-days’ self-isolation rule upon return from abroad. It simplifies control conducted by the police officers and doctors

Owner of the app and portal – the Ministry of Digital Transformation of Ukraine
Data controller – the Ministry of Digital Transformation of Ukraine
Data processor – State Enterprise "DIIA"

Personal data processed via the app:

- full name
- date of birth
- sex
- photo
- cell phone number
- address where self-isolated
- health status
- location
- information on hospitalization or self-isolation if infected



Belarus:
Legal requirements for health data processing in context of new epidemiological requirements

COBALT

New requirements in context of epidemiological situation (1/2)

As Belarus has not announced emergency situation or national quarantine regime, there are no significant COVID-19 related duties of employers in relation to work safety.

Employers had no legal basis for ‘quarantine’ at the enterprise, but many companies have taken measures to isolate workers upon their own initiative.

New requirements in context of epidemiological situation (2/2)

According to the decisions of local administrations of the cities, employers shall take measures to prevent the work of employees with respiratory infections signs, however employers were not provided with legal obligations to monitor the health status of employees and collect relevant data.

Specific requirements are established for (1) hotel business, (2) retail, (3) public catering, (4) providers of social services to population. Such companies shall organize daily temperature measurement and keep the results

Russia:

How employers can observe the new epidemiological requirements without violation of employee privacy?

ALRUD

Situations where written consent is required

Employees' personal data is transferred to the third parties, including affiliates

Company carries out additional activities aimed at protection of its employees' health and safety, e.g. contact tracing

Practical recommendations for employers

Keep new personal data processing activities to the strictly necessary minimum

Avoid or minimize personal data transfer to third parties, including the company's affiliates

Terminate data processing and destroy personal data upon achievement of personal data processing purposes (+30 days) or the term set out by law

Evaluate the possibility of implementing new personal data processing practices without making changes to the existing documentation, obtaining new consents and notifying Russian DPA Roskomnadzor

Make changes to the existing internal policies or adopt new ones while preventive epidemiological measures remain in force, obtain new consents and notify Roskomnadzor if appropriate

ALRUD

What companies are trying to ensure compliance with the GDPR in Russia?

- E-commerce companies
- Banks
- Carriers
- Telecoms operators
- Social networks, etc.

Roskomandzor has confirmed that GDPR may apply to Russian entities

Currently no enforcement actions under the GDPR were taken against Russian companies

Convention 108+ in Russia

Russia signed a protocol modernizing the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dd. 1981

Potential amendments under the Protocol include:

- Data breach notification obligation
- New types of sensitive data
- New roles in data processing (data processor, data recipient)
- Privacy by design principle
- Additional safeguards for protection of personal data
- Strengthening proportionality and data minimization principles

Currently Russian authorities are working on respective legislative novelties

Kazakhstan:

How employers can observe the amendments to the personal data protection legislation and epidemiological requirements without violation of employee privacy?

AEQUITAS
LAW FIRM

Practical recommendations for employers in Kazakhstan

Adopt internal policies related to the protection of personal data or make changes to the existing ones (Regulations on personal data protection, the List of personal data necessary and sufficient for attaining the company's objectives, etc.)

Appoint a person responsible for organizing the processing of personal data

Obtain the consents in writing in the form of an electronic document or by using the service ensuring the safety of personal data or by any other means applying the protective action elements not contradicting the laws

Personal data should be mainly stored in Kazakhstan in any form and on any medium. They can be duplicated and stored outside Kazakhstan in parallel with the primary database existing in Kazakhstan

To elaborate a letter of consent to the collection and processing of personal data. It is necessary to keep personal data processing activities to the strictly necessary minimum

AEQUITAS LAW FIRM

Declarative harmonization with the GDPR in Kazakhstan

Enhanced Partnership and Cooperation Agreement between the European Union and its member states and Kazakhstan (the 'Agreement')

'The Parties shall cooperate in order to ensure a high level of protection of personal data, through the exchange of best practices and experience, taking into account European and international legal instruments and standards. This may include, where appropriate and subject to applicable procedures, accession to, and implementation of, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol by the Republic of Kazakhstan'
(Article 237 of the Agreement)

As of October 2020, Kazakhstan has not yet acceded to the Convention 108. The governmental authorities have not commented on the GDPR application in Kazakhstan, though it remains uncertain

To date, no Kazakhstan companies have faced GDPR enforcement

AEQUITAS LAW FIRM

Ukraine:

How employers can observe the new epidemiological requirements without violation of employee privacy?

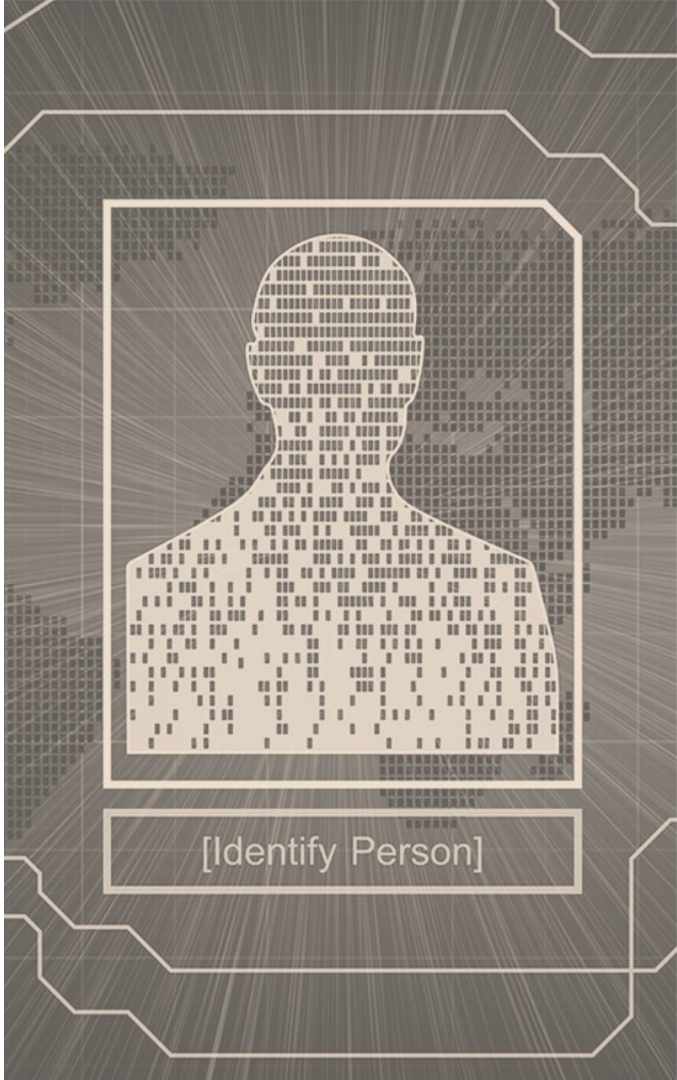
VASIL KISIL

Grounds for sensitive personal data processing

Exercise of the employer's rights and duties in employment relations

Prevention of COVID-19 spread

Explicit consent of the employee



Law of Ukraine dated April 13, 2020, No. 555-IX "On Amendments to the Law of Ukraine" On Protection of the Population from Infectious Diseases" to Prevent the Spread of Coronavirus Disease (COVID-19)"

Practical recommendations for employers

Process only data that is minimally necessary to achieve the purpose

Avoid or minimize personal data transfer to third parties, including the company's affiliates

Erase all data as soon as the purpose is reached, but not later than 30 days after the end of the quarantine period

Notify Ukrainian DPA Ombudsperson only when processing sensitive data not in connection with employer's obligations

Make sure to inform employees about the composition and content of collected data, their rights, the purpose of processing and third parties to whom the data will be transferred

VASIL KISIL

Data protection legislation in Ukraine towards GDPR

- The Ministry of Digital Transformation of Ukraine together with the Parliamentary Commissioner for Human Rights (Ombudsperson) are currently working on a draft law "On Personal Data Protection" that shall meet requirements of the EU standard
- The working group uses experience of leading countries that was analyzed and summarized in the report "Analysis of Legislation on Personal Data Protection of Ukraine" funded by USAID

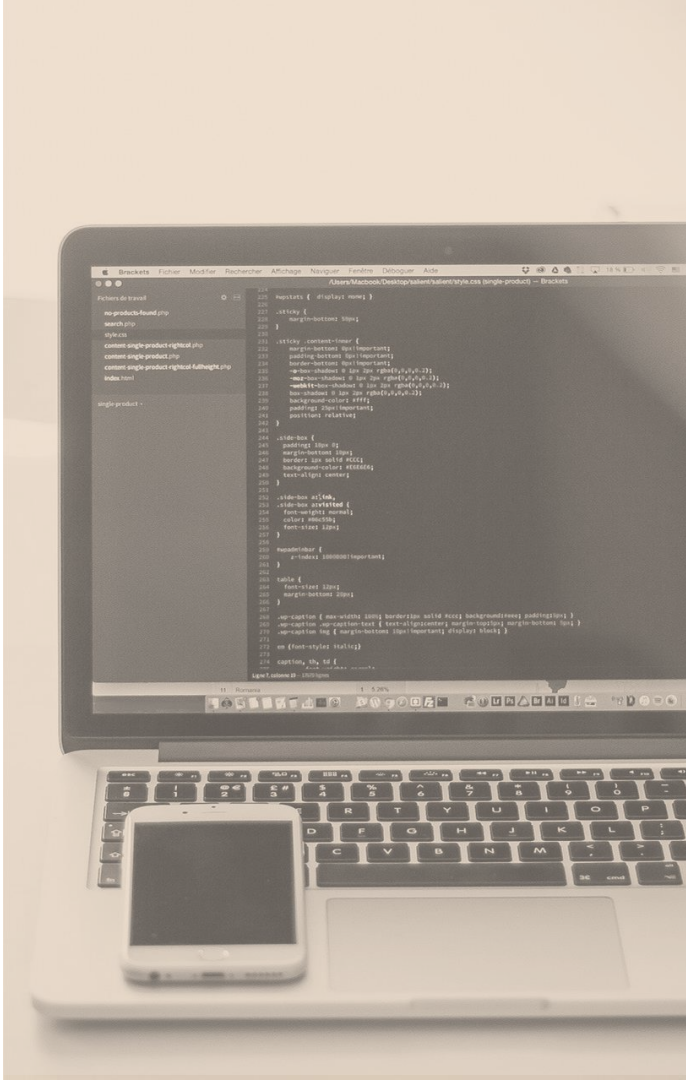
Belarus:

How employers can observe the new epidemiological requirements without violation of employee privacy?

COBALT

Data privacy legislation

- Lack of legislative regulation
- Personal data is considered as basic and additional personal data of an individual, as well as other data which can identify such an individual
- No specific regulation for sensitive/medical data



Situations where written consent is required

According to the Belarusian legislation:

"No one has a right to demand from an individual to provide his personal data […] including information concerning the state of health […] against his will, except for cases established by legislative acts of the Republic of Belarus".

Therefore, collection, processing, storage, transfer to third parties of personal data, shall be carried out upon a written consent of the individual unless otherwise is provided by legislative acts: for example, in case personal data must be disclosed according to law, or is legitimately requested by the bodies conducting administrative or criminal proceedings.

COBALT

Practical recommendations for employers

Legal, organizational and technical measures shall be taken

The legal entity must identify the appropriate departments or officials responsible for data protection

The basis for personal data collection, processing, storage shall be controlled

Make changes to the existing internal policies or adopt new ones if preventive epidemiological measures are taken, obtain consents from employees

COBALT

Russia:

Is it possible to obtain the consent in electronic format?

How the consent can be obtained during remote employment, including in the course of recruiting process?

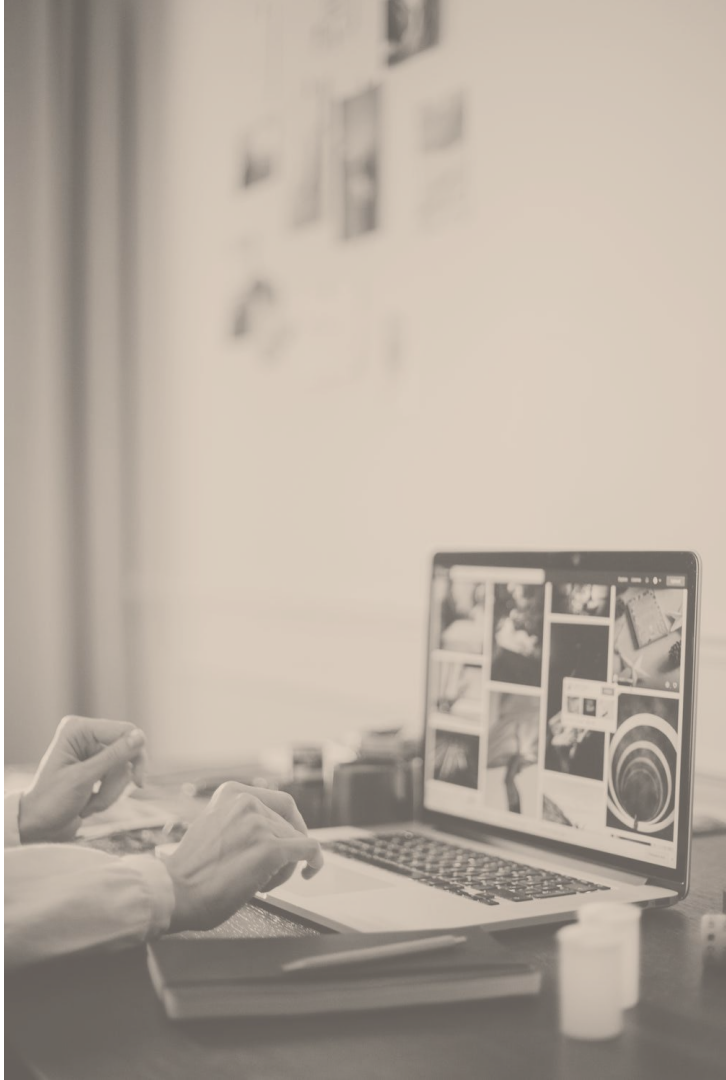
ALRUD

Written consent in electronic format (1/2)

- Consent in the format of an electronic document signed in accordance with the Federal Law "On electronic signature" is considered equivalent to a written consent in hard copy with individual's handwritten signature
- Information in electronic format signed by a simple electronic signature is recognized as an electronic document equivalent to a document in hard copy signed with a handwritten signature in cases established by the Federal Laws or an agreement between the participants of electronic interaction

Written consent in electronic format (2/2)

- Agreements establishing cases of recognition of electronic documents signed by a simple electronic signature as equivalent to paper documents signed with a handwritten signature should provide for the procedure for verifying the electronic signature
- If personal data is processed through an app or a website, it is possible to request a tick-box consent. The respective consent wording should mention a data controller, specify purposes of data processing, and refer to the detailed Privacy Policy



Consent during remote employment, including recruitment

1. When is consent needed? As soon as the employer saves / uploads to its own database or prints the candidate's resume

2. How to obtain a consent? Written consent in hardcopy or through the website by requesting a tick-box consent (except for the cases where written consent is required by law)

3. When to delete an unsuccessful candidate's resume? Upon expiration of limitation period (3 months) + 30 days

Kazakhstan:

Is it possible to obtain the consent in electronic format?

How the consent can be obtained during remote employment, including in the course of recruiting process?

AEQUITAS LAW FIRM

Written consent in electronic format (1/2)

1) Consent in the form of an electronic document signed using electronic digital signature in accordance with the Law On electronic document and an electronic digital signature is considered equivalent to a written consent in hard copy with an individual's handwritten signature

2) "Service ensuring safety of personal data" provides information interaction of owners and / or operators with the individual, including obtainment of the individual's consent to collection and processing of personal data or transfer thereof to third parties, including by way of implementing such interaction independently by owners and/or operators

Written consent in electronic format (2/2)

3) Consent to collection and processing of personal data can be given by any other means applying the protective action elements that do not contradict the Kazakhstan legislation

   The legislation is silent as to the elements of protective actions an owner/operator of the database of personal data may/must apply when obtaining consent to the personal data collection and processing (we recommend personal identification using personal email, phone number, password, pin code, etc.)

Ukraine:

Is it possible to obtain the consent in electronic format?

How the consent can be obtained during remote employment, including in the course of recruiting process?

VASIL KISIL

Written consent in electronic format

- A qualified electronic signature has the same legal force as a handwritten signature and enjoys the presumption of its conformity with a handwritten signature in accordance with the Law of Ukraine "On Electronic Trust Services"
- Consent for the processing of sensitive personal data, if given in electronic format, shall be signed by a qualified electronic signature
- Consent to the processing of other data may be certified by a mere electronic signature (tick-box consent, confirmation by email, scanned handwritten signature, etc.)

Consent during remote employment, including recruitment

- sensitive data – with a qualified electronic signature
- other data – mere electronic signature (including tick-box consent, confirmation by email, scanned handwritten signature, etc.)
- to reproduce consent with mere electronic signature on paper, when possible

During pandemic, the condition of telework may be established in the employer's order without conclusion of an employment contract

Belarus:

Is it possible to obtain the consent in electronic format?

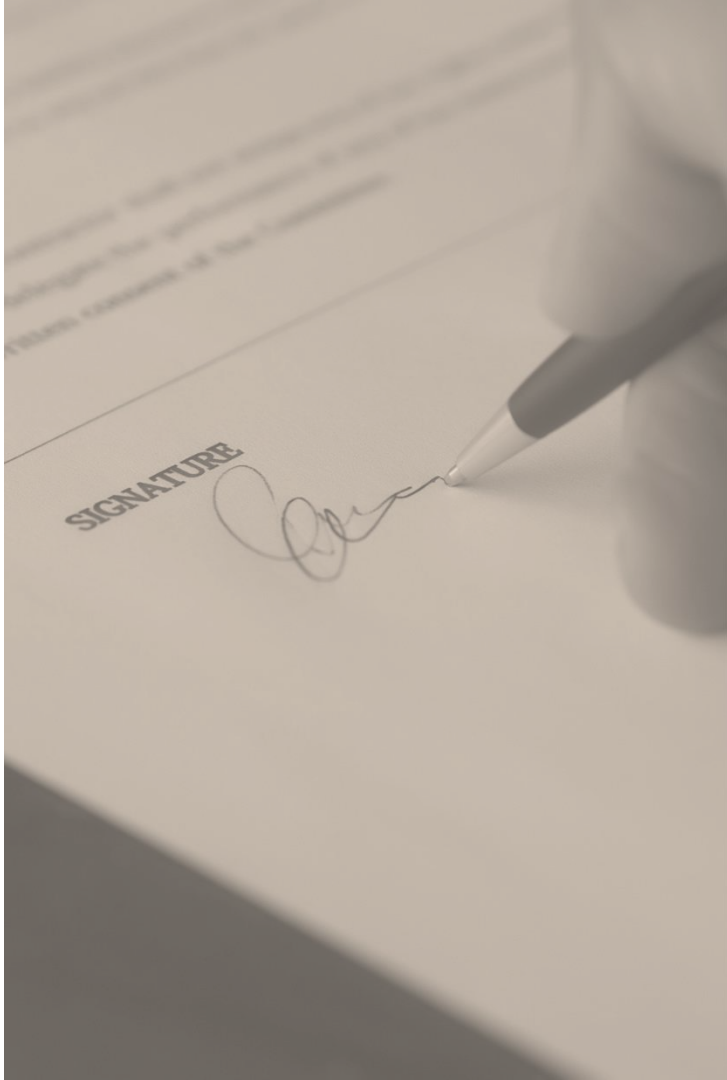
How the consent can be obtained during remote employment, including in the course of recruiting process?

Written consent in electronic format (1/2)

- As a general rule, a written consent of an individual is required. However, the law does not provide clear understanding on how the consent shall be expressed to be considered due
- Consent in the format of an electronic document signed in accordance with the Law "On electronic document and electronic digital signature" is considered due written consent

Written consent in electronic format (2/2)

- Upon agreement of the parties, a simple (not certified) electronic signature can be recognized as due signature, if the procedure for verifying the signatory is established
- It is still questionable if a consent received by such means as tick-box or confirmation by email, etc. can be recognized as due written consent



Russia:
Positions of local regulators and enforcement

ALRUD

Non-provision of information about employees: consequences for employers

- Employers may be administratively liable for violation of the requirements of the Mayor's decrees
- According to the article 20.6.1 of the Code of Administrative Offenses of the Russian Federation, the first offence may entail the warning or the fine up to RUB 300,000 (approx. EUR 3,300) for the companies
- Subsequent offence or offence resulting in harm to human health or property may entail the fine up to RUB 1,000,000 (approx. EUR 11,000) or suspension of activities for up to 90 days for the companies
- Association of Administrative and Technical Inspections of Moscow is responsible for control over compliance with the requirements of the Mayor's decrees. Association's representatives carry out random inspection visits and respond to individuals' complaints

Review of certain issues of court practice related to the application of legislation and measures to counteract the spread of a new coronavirus infection (COVID-19) No. 1 in the Russian Federation" (approved by the Presidium of the Supreme Court of the Russian Federation on April 21, 2020; Decree of the Mayor of Moscow dated April 4, 2020 No. 40-YM

How to organize employee testing for coronavirus?

1. Conclude an agreement with a medical organization on the provision of medical services
2. Compile a list of employees to be tested and notify them to get tested for Covid-19
3. Obtain employees' written consents for their personal data processing and the transfer of information containing medical secrecy
4. Adopt an order for testing implementation
5. To eliminate liability for failure to comply with the requirements of the Mayor's decrees, the employer may request a written refusal to get tested for Covid-19 from an employee

Information from the State Labour Inspection in the Nizhny Novgorod Region, August 7, 2020

First examples of enforcement in the area of data protection

An employee formed a register of persons arriving in Russia, for subsequent transfer to epidemiologists to carry out preventive activities. Later she made a photo of the register and posted it in WhatsApp messenger, thereby violating the confidentiality obligation and provisions of Personal Data Law. An employee received a warning

(Resolution of the magistrate of the judicial section No. 2 in the Liskinsky judicial region dated May 19, 2020, Case No. 5-144 / 2020)

The court took into account the arguments of the employer, who was tried to impute the absence of temperature measurement logs for April-May 2020, since there was no evidence of the absence of the logs during the specified time period. The company claimed that the logs were destroyed as they were filled in and the purpose of processing of employees' personal data was fulfilled

(Resolution of the Novouralsk City Court of the Sverdlovsk Region dated August 21, 2020, Case No 5-237 / 2020)

The employer did not provide information about compliance with preventive measures to the executive and administrative body within 5 days from the date of resumption of activities, did not carry out daily measurements of employees' body temperature in a non-contact way. The company received a warning

(Resolution of the Ilanskiy District Court of the Krasnoyarsk Region dated July, 6 2020, Case No. 5-61 / 2020)

Kazakhstan:
Liability for violation of the legislation in the sphere of personal data

AEQUITAS
LAW FIRM

Liability issues in Kazakhstan

Administrative liability

- Illegal collection and/or processing of personal data
- Violation of the legislation on informatization committed in the form of a failure to implement or improper implementation of measures to protect information systems containing personal data

Criminal liability

- Illegal collection of information about private life of a person that constitutes his/her personal or family secret without his/her consent or causes *substantial harm* to the rights and lawful interests of that person
- Illegal distribution of electronic information resources containing personal data of citizens or other information where access to such information is limited by laws or by the owner
- *Where a failure to comply with legislative requirements entails substantial damage*

Civil liability

- Civil claims of personal data subjects related to harm caused by unlawful processing of their personal data

AQUITAS LAW FIRM

Ukraine:
Positions of local regulators and enforcement

VASIL KISIL

Ministry of Health of Ukraine

The employees must control their temperature themselves before the start of the shift / working day. They must also take care of wearing a mask indoors, and washing their hands regularly

Parliamentary Commissioner for Human Rights (Ombudsperson)

2020 strategic goal – monitoring activities of debt collection agencies regarding personal data protection requirements

Audits in the field of healthcare: inspections of medical centers and laboratories conducting COVID-19 testing

Inspection of the Ministry of Digital Transformation and SE "DIIA"

VASIL KISIL

Employers' liability for violation of personal data protection and quarantine rules

- Directors may be administratively liable in accordance with Article 44^3 of the Code on Administrative Offences (violation of quarantine rules) with a fine from UAH 34,000 (approx. EUR 1,020) up to UAH 170,000 (approx. EUR 5,100)
- Directors may be administratively liable in accordance with Article 188^{39} of the Code on Administrative Offences (violation of personal data protection rules) with a fine from UAH 3,400 (approx. EUR 100) up to UAH 34,000 (approx. EUR 1,020)
- Any person may be criminally liable in accordance with Article 182 of the Criminal Code (gross violation of privacy) with a fine from UAH 8,500 (approx. EUR 250) up to UAH 17,000 (approx. EUR 500)

VASIL KISIL

Belarus:
Positions of local regulators and enforcement

COBALT

Positions of local regulators and enforcement

No official position of authorities regarding data privacy, in particular in the context of epidemiological situation

Administrative liability is established for intentional unlawful disclosure of personal data by a person to whom personal data is available in connection with professional activity, in the form of a fine up to appr. 180 EUR

Criminal liability is also established for illegal collection or distribution of information about private life in the form of community service/fine/arrest

However, as of yet, practice of its application to cases of unlawful disclosure of personal data is not available

! Draft Law on Personal Data passed in its first reading in 2019 and currently is on pause. After its adoption and official publication, a supervisory authority responsible for data protection shall be established

COBALT


Questions?

Speakers

Anastasia Petrova

Senior Associate

ALRUD, Russia

apetrova@alrud.com

P: +7 495 234 96 92

Anastasia Bykowskaya

Managing Associate

COBALT, Belarus

anastasia.bykowskaya@cobalt.legal

P: + 375 29 624 59 15

Oleksandr Melnyk

Senior Associate

Vasil Kisil and Partners, Ukraine

melnyk@vkp.ua

P: +38 044 581 77 77

Yekaterina Khamidullina

Senior Associate

AEQUITAS, Kazakhstan

y.khamidullina@aequitas.kz

P: +7 (727) 3 968 968

Thanks for your attention