STATE
INSPECTOR'S
SERVICE

STATEMENT OF THE STATE INSPECTOR'S SERVICE

Recommendations on personal data protection in the course of fight against **Covid-19 (Coronavirus)**

2020 YEAR

Norwegian Ministry
of Foreign Affairs

U N
D P

*Empowered lives.
Resilient nations.*

This publication has been produced with the assistance of the Norwegian Government and the United Nations Development Programme (UNDP). Its contents are the sole responsibility of the State Inspector's Service and do not necessarily reflect the views of the Norwegian Government and the United Nations Development Programme.

ALONG WITH THE RAPID SPREAD OF THE COVID-19 OUTBREAK, THERE IS GROWING PUBLIC CONCERN ABOUT PERSONAL DATA PROTECTION IN THE COURSE OF FIGHT AGAINST THE VIRUS.

In this regard, the State Inspector’s Service elaborated recommendations for dealing with personal data protection during the pandemic. These recommendations are intended to assist organizations in managing personal data and confidential information.

THE ISSUES INTERPRETED IN THE RECOMMENDATION ARE AS FOLLOWS:

- Personal data processing by healthcare institutions
- Processing the data of employees by employer organizations
- Distance learning and meetings
- Data processing while working remotely

სახელმწიფო ინსპექტორის სამსახური
STATE INSPECTOR’S SERVICE

PERSONAL DATA PROCESSING BY HEALTHCARE INSTITUTIONS

Public health institutions, in accordance with the existing legislation, collect and process various personal data necessary for managing and functioning of the health care system.
In the fight against the spread of the virus, healthcare institutions have to collect data of the infected and/or possibly infected individuals to a greater extent than in standard cases (for instance, they collect information on citizens traveling abroad, workplace, persons in close contact with them), that results from existing needs and does not contradict legislation.

In order to keep the public informed about the pandemic and to provide medical consultations, it is allowed to send informational messages via telecommunication and latest technologies.

It should be borne in mind that in such situations, the risk of receiving misleading and “fraudulent messages” increases. Therefore, it is important that citizens rely solely on the information received from official bodies.

Public disclosure of the identity (name, surname) of persons infected/possibly infected with the virus and/or of those in contact with them, is usually unnecessary. For reasons of public interest, it is sufficient to disseminate information about them in a non-identifiable manner (citizenship, ethnicity, age, workplace, route of displacement etc.). Identity disclosure to public and third parties shall be permissible to the extent that is necessary for the prevention, control and management of the disease.

PROCESSING THE DATA OF EMPLOYEES BY EMPLOYER ORGANIZATIONS

In addition to providing safe environment for employees, employers strive to maintain continuity of business.

According to the legislation, employers are allowed to collect information on infecting of employees regardless of their will if it serves to provide a safe working environment and/or to manage the healthcare system.

An employer may collect the following information: whether the employee visited a high risk country affected by the virus, whether the employee has symptoms of the virus, or if he or she had contact with the person(s) infected with the virus.

If an employee is suspected of being infected, the employer should contact relevant healthcare authority and be subject to its instructions.

An employer may disclose information on the infection of the employee to other employees if this is necessary to identify the person in contact with the infected and/or to prevent further spreading of the virus.

The data obtained by an employer shall be kept for the period necessary to carry out the activities falling within its competence. Subsequently, such data shall be deleted, destroyed or stored in an anonymous form.

DISTANCE LEARNING AND MEETINGS

Educational Institutions (schools, universities) have turned to distance learning. Remote meetings are also held frequently.

Photo-video (including humorous) content of distance learning process and online meetings are disseminated in social media. This material from online learning and meetings includes personal data and should be considered when the content is made public.

Disclosure of minors' data in an accessible form to anyone on the Internet may have an adverse effect on the minor (becoming the object of bullying or other form of undesirable treatment).

Consequently, educational institutions, those employed in these institutions, as well as parents and family members of minors, should be more responsible with respect to publicizing children's' data and acting in the best interests of the minor.

Modern collaborative communication systems (for example, Webex, Zoom, Teams, etc.) may be used to set up remote meetings.

Webex Meetings

zoom

Microsoft Teams

სახელმწიფო ინსპექტორის სამსახური
STATE INSPECTOR'S SERVICE

DATA PROCESSING WHILE WORKING REMOTELY

Most organizations have already turned to remote working mode. Latest technologies have made remote work easy, but the issue of confidentiality and security of business information is on the agenda during such times.

THE FOLLOWING SHALL BE TAKEN INTO ACCOUNT WHEN WORKING REMOTELY:

- It is advisable to use an office computer while working remotely from home;
- If remote access from personal computer to office computer is needed, modern and up-to-date programs shall be used;
- Operating systems (MS Windows, MacOS) shall be regularly updated on personal computer;
- It is necessary to set a computer login password;
- It is best to use a complex password (containing at least 10 characters, uppercase and lowercase Latin letters, digits, and special characters. i.e. #, $, &, @, etc.) for accessing electronic systems that can be accessed by an individual username. In addition, where possible, two-factor authentication mechanisms (password and additional one-time code in addition to username) shall be used;
- The same password shall not be used for logging into different systems;
- Only encrypted VPN connection means shall be used to access internal electronic resources of the office;
- Antivirus programs, even free versions, shall be used;
- It is advisable to back up data or save important documents and data to the server of the office;
- Confidential data shall be encrypted, even using free encryption programs (for instance, VeraCrypt, BitLocker, etc.);
- No external USB data carriers shall be used;
- Physical security of a computer shall also be protected (the employee shall not leave it unattended in different places).

სახელმწიფო ინსპექტორის სამსახური
STATE INSPECTOR'S SERVICE

THE EMPLOYEE MUST ENSURE THE SECURITY OF HOME WIRELESS NETWORK DEVICE AS WELL. NAMELY:

- ✓ User password assigned to manage home wireless network device shall not be known to anyone else;
- ✓ If possible, it is best to limit access to control panel of wireless network device from the Internet;
- ✓ Encryption methods used for wireless network connection shall preferably be up to date (for example, WPA2 or WPA3);
- ✓ Password connecting with home wireless network device shall be complex and not less than 16 characters long;
- ✓ Password for connecting a wireless network device must be changed periodically.

In addition, it is worth noting that hackers take advantage of the pandemic situation.

Many false, so-called “phishing” websites are created where the statistical data on the spread of the virus are placed and access to which can afterwards result in having the data stolen from computers. For this reason, it is recommended to only view the statistics on the official websites or on websites of news agencies and media outlets.

In addition, there is a major increase in sending e-mails with false, so called “phishing” letters/texts. False messages are sent on behalf of well-known organizations or individuals in order to steal confidential or personal information.

Files enclosed to emails sent by unknown organizations and individuals also carry risk. Therefore, the attached files should not be opened until the user is convinced of the reliability and credibility of the sender organization and/or individual.

STATE
INSPECTOR’S
SERVICE