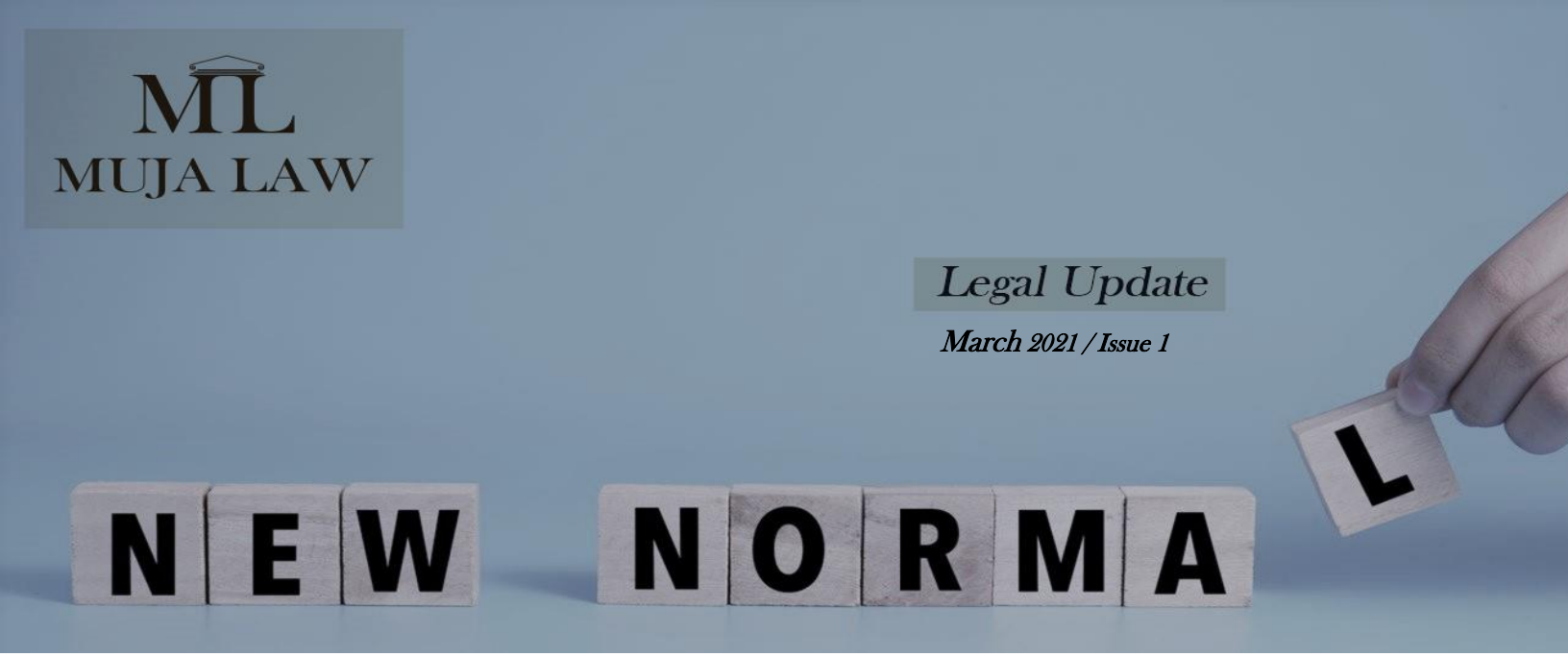
MUJA LAW

Legal Update

March 2021 / Issue 1



Muja Law brings you that latest issue of the *Legal Update*.

Recently the Office of the Commissioner for the Right to Information and Protection of Personal Data in Albania (hereinafter referred to as "*Office of the Commissioner*"), has approved a new guide on personal data processing during telework (hereinafter referred to as "*the Guide*") within the measures against COVID-19.

The Guide brings to the attention of each interested party some specific aspects regarding the protection of personal data during telework, from the situation created by the pandemic caused by the spread of the COVID-19 virus.

Also, the rules in this Guide are based on the Labour Code of the Republic of Albania, which has provided telework as work that the employee performs at home, or in another place, defined in agreement with the employer, using technology of information and communication, within the working time according to the conditions agreed between them in the employment contract.

Some of the most important aspects of the Guide are as follows:

The Guide

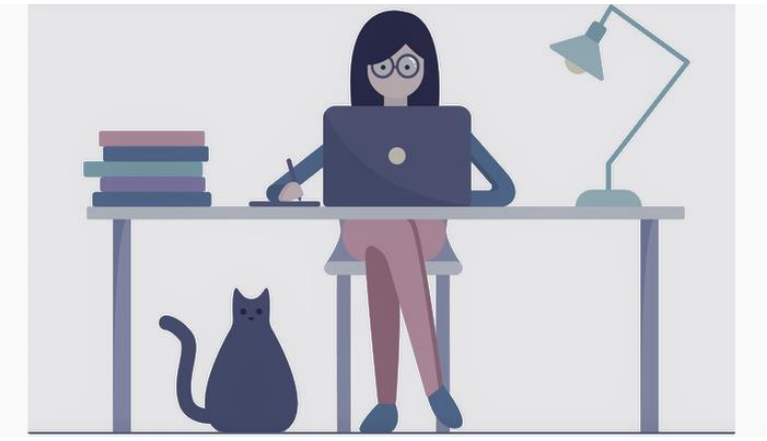
The Guide provides that respect for human dignity, privacy and protection of personal data must be guaranteed in any data processing for employment purposes, to allow the free development of the employee's personality, as well as to create opportunities for the development of individual and social relations in workplace.

Due to the situation caused by the spread of the COVID-19 virus, employers (*controllers*), in order to continue their activity, have seen as an alternative the use of telework as an efficient way in such situations. Consequently, there is a need to orient controllers and data subjects on issues of guaranteeing standards of storage, processing and security of personal data.

❖ Understanding Telework. Processing of personal data by the employer through teleworking

The Guide provides that teleworking is a form of work organization, which does not take place in the employer's workplace, but in other work environments using information and communication technology tools. The rights of the employer formalized in the employment contract and specific legislation, must be exercised in compliance with the right to privacy and personal data.

In virtue of the Guide, the employer must justify the implementation of the measures, which must be proportionate to the intended objective. The processing of personal data by the employer must be carried out in accordance with the principles and criteria set out in the law on personal data protection.



Employers during the monitoring must respect the principle of data adequacy according to the law on personal data protection, which provides that: "*Personal data can be collected only if it is necessary to achieve a specific purpose and not to exceed this purpose*". To prove this, they will need to assess in advance whether the collection of employees' personal data is proportionate to the purpose. In this view, it should be assessed by the employer whether there is another less intrusive way of privacy in which the same results can be achieved.

The employer must also ensure that it informs in a particularly clear and complete manner about the categories of personal data that may be collected through information technology tools, according to the law on personal data protection.

Information should be provided in the fullest possible way, in an accessible and up-to-date format. In any case, such information must be provided before an employee can perform the relevant activity or action and be made immediately available through the information systems commonly used by the employee.

Regarding the monitoring of employees, the Guide provides that each employer (controller) must consider in advance some legal criteria before starting the process of personal data processing. According to the law on personal data protection, any processing of personal data must have a specific, clear and lawful purpose. A legitimate purpose for employee monitoring may be, for example, maintaining the security of personal data when employees work remotely, ensuring compliance with legal obligations or ensuring that an employee is performing his or her obligations under an employment contract. Once the legitimate purpose of the processing has been clearly identified, the employer must ensure that any personal data collected for that purpose is processed only as necessary for that specific purpose, in accordance with the principle of purpose restriction. *The key to this procedure will be to ensure that the monitoring proposed by the employer is within the reasonable expectations of the employees.*

It is recommended that employers consult with employee representatives, in accordance with specific legislation or the collective

agreement signed with the latter's unions (if any), before applying any monitoring system, including cameras. This principle is followed even in cases when changes are foreseen in the process or the way of monitoring the employees.

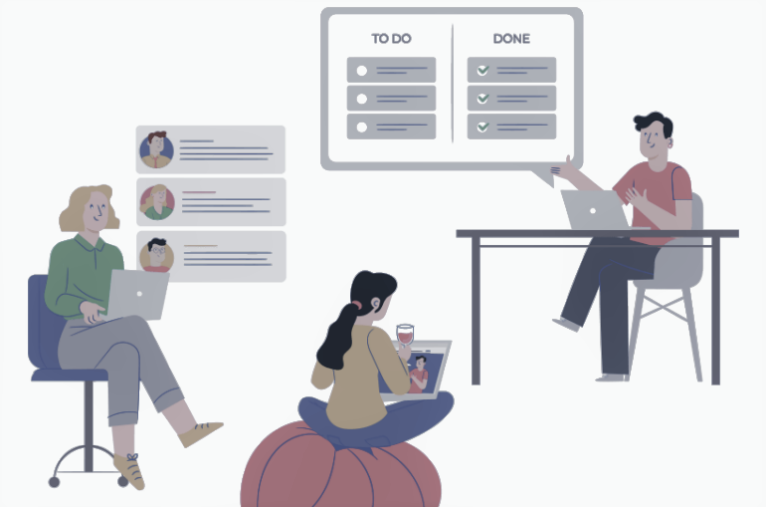
Referring to the provisions of the law on personal data protection, regarding the supervision of employees during the telework process, it is not possible for employers to rely only on consent as the legal basis on which they process their personal data, due to the imbalance of power in relations between employers and employees, which makes it difficult to prove that consent was given freely. According to the provisions of law on personal data protection "*Consent of data subjects*" is "*any written statement, given expressly with full and free will and being fully aware of the reason why the data will be processed, which means that the data subject agrees to have his data processed*".

The legal processing criteria will, however, depend on the specific situation and may be, when the processing of personal data through monitoring is necessary for the performance of the employment contract, or is necessary for the observance of a legal obligation to which the employer is subject, or it is necessary for the purposes of the legitimate interests of the employer (*when this is not violated by the fundamental rights and freedoms of the employees*). So, it should be applied one of the legal processing criteria set out in law on personal data protection.

To ensure that potential risks to privacy are minimized through employee monitoring, the Guide provides that a data protection impact assessment should be conducted in advance, in cases where processing "*is likely to result in a high risk to rights and individual freedoms*". Employee monitoring reaches this limit, especially when there is systematic monitoring, when new technologies are used that have an impact on privacy, or an assessment is being conducted based on monitoring their performance.

❖ The rights of the employee in the capacity of personal data subject

Employees, in the capacity of personal data subjects, can exercise the rights they enjoy under the legislation on personal data protection even during telework, such as the right of access, the right to request blocking, correction or deletion, the right not to be subject to automatic decision-making, the right to object and the right to appeal.



Exceptions to the rights mentioned above can be allowed if provided by the law on personal data protection and other specific legal acts that regulate the employment relationship (*this also depends on the field of employment*), or are a necessary measure in a democratic society, to protect the interests of national security, public safety, foreign policy, economic and financial interests of the state, the prevention and prosecution of criminal offenses, the protection of the data subject or the rights and freedoms of others.

Employers must continue to protect the rights of their employees, ensuring that any

request made by the latter is handled properly and efficiently by the persons in charge, such as the Contact Person for the Protection of Personal Data.

Regarding personal data protection, the Guide provides that employers must provide specific training for their employees. Also, they have the obligation to update their internal guidelines/regulations, in terms of access and processing of personal data within the employment relationship in the new conditions of work organization.

Employers should be engaged in informing employees about the use of data processing mechanisms within telework (such as video conferencing, etc.) and measures to ensure the security of personal data.

Employers should also in any case inform employees about new ways of monitoring and processing personal data, as well as provide practical guidance on the use of electronic devices in a proper and safe manner. Employers may instruct employees on how and when video conferencing will be permitted, specifying the limitation of their systematic recordings and the sharing of such recordings with unauthorized third parties. Employers must provide understandable and accurate information to employees about the mechanisms (settings) that such devices provide, to ensure data security.

❖ Data security measures

The situation created by COVID-19, brought as a need the widespread use of telework. This situation can potentially lead to possible deviation from standard work processes and difficulty in securing automated tools during teleworking, so there is a higher possibility of personal data breaches due to human error.

Applying for the first time or increasing the use of telecommunication tools may raise the issue of taking additional measures related to data security.

In this context, the Guide provides that employers should draft rules regarding data security in the framework of telework, which must be respected, in accordance with the provisions of the law on personal data protection, as well as draft an information document within telework, in order to make it available to employees for those to be recognized and put into practice.

As part of these measures, the employer must make available to employees a list of communication equipment/tools or group work, to be suitable for distance work. They must guarantee the confidentiality of personal data and information transmitted and accessed by employees, e.g., the use of a VPN to avoid direct exposure to online services.

Some practical measures that can be taken to keep personal data safe and confidential while working outside the office are:

- Regarding equipment:

- Ensure that every device has the necessary updates, such as operating system updates (such as iOS or Android) and software and antivirus updates;
- Securing the computer, laptop or device in a safe location;
- Taking care not to lose devices such as

USB, phones, laptops or tablets;
- Locking the device if there is a need to leave it unattended for any reason;
- Ensuring that equipment is turned off, locked or stored carefully when not in use;
- Using effective device access controls (such as multi-factor authentication and strong passwords) and where necessary, encryption to restrict access to the device and reduce the risk of a device being stolen or moved;
- When a device is lost steps should be taken immediately to ensure remote memory erasure, where possible.

- Regarding Emails:

- Following the same policies applied in the institution or company, regarding the use of e-mail;
- Using work email accounts, instead of personal ones. If personal e-mail is to be used make sure that the content and information or attached documents are encrypted;
- Before sending an e-mail, making sure they are being sent to the correct recipients, especially for emails that contain large amounts of personal data or sensitive data.

- Regarding Cloud and network access:

- Where possible, using only the institution's trusted networks or Cloud services, and in accordance with organizational rules and procedures relating to cloud or network access, data access and dissemination;
- If one is not working in the cloud or without network access, making sure that any processed data is stored appropriately and securely.

The Guide provides that the above measures should be taken in the framework of the implementation of Instruction no. 47, dated 14.09.2018, "*On determining the rules for maintaining the security of personal data processed by large processing entities*" and Instruction no. 48, dated 14.09.2018, "*On the certification of management systems of information security, personal data and their protection*", approved by the Office of the Commissioner.

❖ Integrity and confidentiality

Employees, while teleworking, often use their personal devices (computer, laptop, smart phone) for professional purposes and rely on VPN connections to remotely access companies' IT systems, which can lead to increased risk for employers.

As for the above, the Guide provides that the employer must implement appropriate safety measures and may need to update safety policies and other internal documentation to address specific issues such as work from home and BYOD. *The use of personal computer devices in a professional context is known by the acronym "BYOD", which is an abbreviation of the English expression "Bring Your Own Device".* BYOD itself is not "personal data processing", but a special technical tool on which processing is based.

The use of personal equipment depends on the choice of the employer, who may simultaneously authorize this with certain conditions, or prohibit it altogether.

Employers should inform employees of the existence of these risks (such as computer hackers sending fake emails, known as phishing emails or spam), because the loss, destruction or unauthorized access to personal data, regardless of whether it is accidental or unintentional, is considered a violation of personal data by law.

❖ How to reduce these risks?

The following are some practical measures that can be applied in this case:

- Isolating parts of personal equipment that are likely to be used in a professional setting;
- Controlling access remotely through a set of user authentication measures (if possible, via an electronic certificate, SIM card, etc.);
- Applying information traffic coding measures (VPN, HTTPS, etc.);
- Requiring compliance with basic security measures such as locking the device with a password in accordance with good practice and using an updated antivirus;
- To make users aware of the potential risks, formally separating responsibilities for each and to specify the preventive measures to be implemented in a binding document.

❖ Processing of personal data and monitoring of employees through cameras

There is a tendency of public and private employers (in the quality of controllers) to monitor employees within the employment relationship, using different mechanisms, ways and means. A very common way of monitoring is through cameras.

The principle of adequacy of personal data, provided in law on personal data protection, means the fact that controllers (public or private) must collect and process personal data in accordance with the purpose of processing and not exceed this goal.

Similarly, the employer should assess whether it is proportionate to collect data in relation to the timing and frequency of employee leave to monitor their work from home, what data is needed to ensure the security of the employer's information systems. (e.g., activating the device camera, recording mouse movements, screen shots), etc.

Monitoring the employee for the purpose of supervising the work, through the video surveillance system (CCTV), is in principle prohibited. Cameras cannot be used to monitor an employee in the workplace. Placing cameras in the employees' working environments, office or home in order to monitor or evaluate performance is in principle contrary to the provisions of law on personal data protection and the bylaws, namely Instruction no. 11, dated 08.09.2011, of the Commissioner on "*Processing of personal data of employees in the private sector*", as amended.

Meanwhile, the use of CCTV (working device camera) in order to communicate with the employer during telework is in the latter's assessment. It is in the competence of the employer (controller) to determine the purpose and the ways of data processing, in function of his activity, respecting the provisions of the legislation on personal data protection.

Some video conferencing platforms allow event managers to analyze the attention of their participants in real time while others allow recording of meetings. Such recordings may include participants' voice, messaging communications, faces, private home environment (captured via webcam) as well as the screen shared by the speakers. Some other websites enable automatic transcripts.

In principle, employers should not force camera activation on employees attending video conferencing.

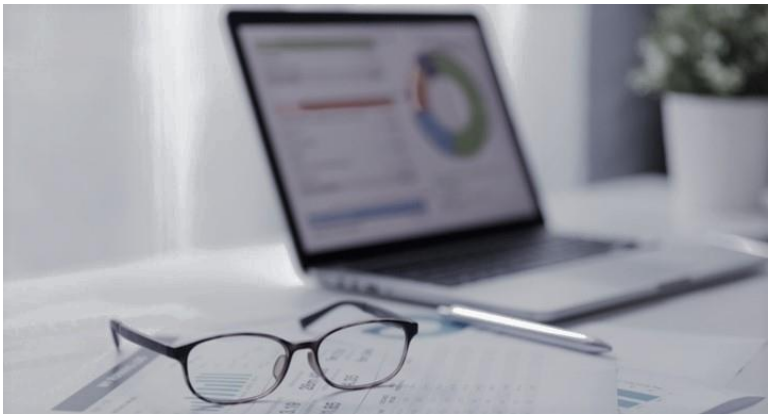
Telework can violate the right to respect for privacy, especially of other persons present in the apartment. *For this reason, an employee may in principle refuse to transmit his images during a video conference, stating the reasons relating to his particular situation.* Only in very special circumstances, which are for the employer to define and justify, can face-to-face video conferencing become necessary.

Also, the employer may not use a permanent supervision device. If the employer has the right to control the activity of his employees, he cannot place them under permanent supervision, except in exceptional cases, which must be duly justified in relation to the nature of the duty of the employee.

❖ Physical registers/written documents

It is important to note that personal data protection, during teleworking, applies not only to electronically processed personal data, but also to manually processed (hard copy) personal data.

The Guide provides that during teleworking, the use of papers or documents must be accompanied by the undertaking of specific measures by the employer to guarantee their security and confidentiality. Specific documents that may be taken out of the workplace should be kept to ensure that they are not lost or accessed by unauthorized persons. Where possible, the employer should keep written records of which documents were obtained at home.



If you wish to know more on our publications, legal updates, tax updates, legal bulletins, or other articles, you may contact the following:

contact@mujalaw.com

Muja Law Office
Rr. "Ibrahim Tukiqi", Nr.2
1057 Tirana
Albania
Mob: +355 69 28 28 562
Web: www.mujalaw.com

Muja Law is a family-run law office where we work hard for the success of our clients and to provide excellence in legal service. Our roots go back to 2001 when our Managing Partner, Krenare Muja (Sheqeraku), opened her law practice office in Tirana, Albania. Krenare's son Eno joined her in 2014, and the other son Adi entered the practice in 2019. What started in Tirana as a small, family-run law office has grown and flourished in the community for the last 20 years. The office consists of various respected and talented lawyers who possess outstanding educational and community service backgrounds and have a wealth of experience in representing a diverse client base in various areas of the law.

The office is full-service and advises clients on all areas of civil, commercial and administrative law. With significant industry expertise, we strive to provide our clients with practical business driven advice that is clear and straight to the point, constantly up to date, not only with the frequent legislative changes in Albania, but also the developments of international legal practice and domestic case law. The office delivers services to clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods. In our law office, we also like to help our clients with mediation services, as an alternative dispute resolution method to their problems.

While we have grown over the past 20 years and become recognized as one of Albania's leading law offices, we are grounded in the essence of "who" we are and "where" we started. We understand the importance of family, hard-work, and dedication.

MUJA LAW