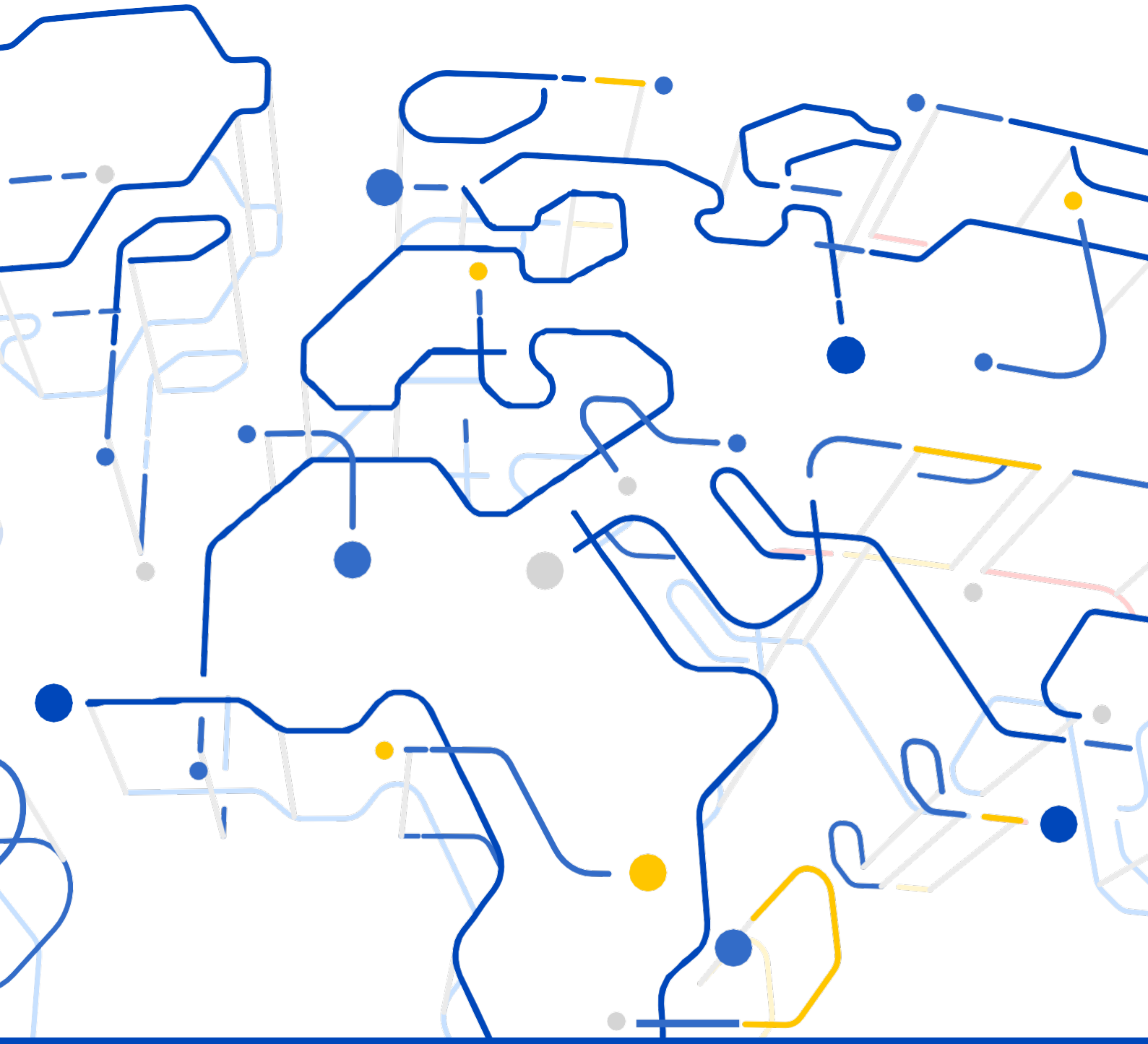

Adriala: Covid-19 Comparative Legal Guide:
Processing of personal data in the context COVID-19

adriala

ALBANIA - BOSNIA AND HERZEGOVINA - BULGARIA - CROATIA - KOSOVO - NORTH MACEDONIA - MONTENEGRO - SERBIA - SLOVENIA

ALBANIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Albania

The Albanian Commissioner for the Personal Data Protection (the "**Data Protection Commissioner**") has issued new guidelines in the context of Covid-19 outbreak.

For the time being the Albanian authorities haven't introduced novel contact tracing or similar technologies/apps, therefore we don't note any changes to the current personal data protection legislation and practice.

The Data Protection Commissioner has invited the data protection controllers, such as mass media, employers or competent authorities to use any personal data collected in line with the current legislation and all practices.

Does the applicable law in Albania allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

The Data Protection Commissioner has confirmed in the most recent guideline that employers' control on their employees' health conditions is not in collision with the Albanian legislation on personal data protection in force, in the context of the Covid-10 outbreak.

Nevertheless, the Data Protection Commissioner has emphasized that such controls must be made (i) in compliance with their scope and must not be disproportionate, (ii) in the least invasive manner (iii) through the adequate means in order to assure the protection of all such data and (iv) after the end of the pandemics, all such data must be deleted and standard practices must be duly restored.

It would be at the discretion of employers to take all the appropriate measures to ensure the duly implementation of the principles governing the personal data control per the Albanian Data Protection Commissioner.

Does the applicable law in Albania allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

Pursuant to the recent guidelines of the Personal Data Commissioner, employers must take all possible measures to ensure that working from home does not affect the personal data protection rights granted to employees by the Albanian legislation in force.

In the light of the above and taking into consideration the legal provisions of the

Albanian Labor Code on teleworking, we understand that consent from employees may be required for the use of personal devices, unless the employer has already supplied employees with working tools for the purpose of working from home.

Anyhow, we are of the opinion that employees must not unreasonably refuse to use their personal devices, as long as teleworking enables both parties to keep performing their contractual obligations under the employment agreement under the extraordinary circumstances caused by the Covid-19 pandemics and that it is more than common for the market participants to use their personal mobile devices such as mobile phones during the ordinary course of daily work. In addition, any requests from the employer to employees to work from home through their personal device is proportionate and reasonable in the context of the Covid-19 pandemics.

Does the applicable law in Albania allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

Based on the Albanian Personal Data Protection Commissioner guidelines referred to herein above, the same principles would apply as well.

This means that all transfer of the personal data must be made (i) in compliance with the scope for which the data are being collected/processed, (ii) such processing must be proportionate, (iii) in the least invasive manner, and (iv) through the adequate means in order to assure the protection of all such personal data from any unauthorized transfer, procession or disclose to unauthorized parties, in line with the current Albanian legislation and market practice.

Anyhow, international transfer of personal data is subject to the current regulation, which allows for automatic transfer in case data are transferred to countries with adequate security measures, identified and approved by the Personal Data Commissioner (i.e. EU/EEA countries, etc.). Otherwise, the consent of the subject whose personal data are being transferred would be required.

BULGARIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Bulgaria.

There are three major issues raise by the implementation of the state of emergency because of COVID-19.

Declarations collected by the Ministry of Interior

The Ministry of Interior collects and processes declarations for two purposes. One is arrivals from abroad, where each passenger must declare (in addition to 'standard' personal date for declarations) the address of residence and provide their mobile numbers to receive calls by the police, where he or she will spend the mandatory quarantine after arrival. The police collect these declarations and performs occasional checks at the designated addresses (failure to appear may result in prosecution).

Further, because of restrictions on intercity travels, the police collect declarations for (among other information) the purpose of such travel (which include employment data, health status data, etc.).

The Bulgarian COVID Act provides for the army to assist the police on demand in such checks.

On 25 March 2020 the Bulgarian Personal Data Protection Commission (BPDPC) has issued a letter to confirm such actions by the police (presumably this shall extend to the army, if involved) is justified for reasons of public health and crime prevention. BPDPC takes the view that regulation (EU) 2016/670 allows to restrict the rights and the liberties of citizens in such circumstances. BPDPC invites citizens to rest assured that such restrictions are not in breach of their rights and liberties. BPDPC also states that such emergency does not release the police from the duty to process personal data only for the purposes of the state of emergency and upon implementing adequate protection measures. However, BPDPC does not clearly instruct the police when to destroy the personal data collected.

Location of mobile devices

The Bulgarian COVID Act introduces an obligation of the telecom operators to provide their data on location of mobile devices and calls to the police. Such measure was heavily debated at the Parliament but adopted. There was a precedent of a person, who boasted on Facebook that he is not at the address specified in the declaration, completed upon arrival and he was arrested, relocated and is being prosecuted. BPDPC has not (yet) commented on the process of such personal data. Presumably, if they do, will take similar view as thy took on declarations.

Age and Family Issues

Certain orders of the minister of public health 9who is delegated to issue mandatory orders under the COVID Act) raise other issues, such as:

- There is a 'green corridor' for elderly people (60+) to shop between 09.30 and 10.30. While generally it is a matter of 'face control', a proof of eligibility requests identification to shops personnel. Further, some understand this as prohibition for elderly to shop for the rest of the day, which enhances the discrimination potentials.
- It is prohibited for more than 2 persons to meet in public and there is no exemption for families. At some shop's doorkeepers would not allow a family to walk in together.

Other concerns

- Briefings in the media on current situation in the country include disclosure of the gender, residence, travel data and professional or family data (although on no name basis). Especially in smaller towns, persons can be easily identified.
- It was just disclosed that there is electronic exchange platform between hospitals and medical administration , which apparently is not exactly cleared in terms of GDPR, it is likely that an app to include self-reporting, including location will be offered, which could be integrated with the said platform.
- Where volunteers offer help to elderly people with no relatives (typically purchase of foods and medicines) so that they could stay home, technically such humane actions entail collection and processing of personal data (even where beneficiaries call).
- Taking care of a relative, resident in another town or village is subject the above-mentioned declarations and travel restrictions and include disclosure of a third person personal data.

These restrictions appear justified but have not (except for the declarations) been commented upon by the BPDPC.

CONTACT: info@adriala.com | www.adriala.com
Albania | Bosnia & Herzegovina (Banja Luka & Sarajevo) | Bulgaria | Croatia | Kosovo | Montenegro | North Macedonia | Serbia | Slovenia

CROATIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Croatia.

Please note that this short guide is for informative purposes only and provides only general guidelines and remarks on the processing of personal data in the context of the COVID-19 pandemic. It does not represent legal advice in any capacity.

Does the applicable law in Croatia allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

The processing of data related to health is not specially considered in Croatian personal data protection legislation, thus the rules set out in Article 9 of the GDPR apply.

As stated by the Croatian Data Protection Agency, employers have a basis for processing health data of employees in the Croatian Employment Act and Occupational Health and Safety Act, which mandate employers to undertake adequate measures to protect the health and safety of their employees, which is also recognized as a basis for processing under Article 9 section 2 point b) of the GDPR.

However, in line with the general requirement of data minimization and the proportionality of the intrusion of an individual's privacy to the necessity of the processing, the legality of tracking body temperature and COVID-19 infection has to be evaluated on a case by case basis, taking into account the type of business the employer is in, the organization of work and other factors which affect the effectiveness of preventative measures.

In case the employer can legally process the health data of employees, it is also necessary to consider the means and duration of storing that category of data. One possibility is that the employer chooses not to keep any records of such data at all, and where it is inevitable to record it, to record it using proper organizational and technical measure to protect said data, and to keep it only for very short periods of time, after which it should be permanently deleted. Further processing of such data, and especially forwarding it to third parties or other individuals within the employer's organization is out of the question.

Even though processing of health data can be based on consent, in this case the validity of an employee's consent can be rightfully questioned due to the imbalance of power between the data controller and the data subject which is inherent to the employer-employee relationship, especially in the current state of economic crisis where the employee's position is further weakened.

Employers are additionally obligated to stay informed on any decisions of the Civil Protection Authority and undertake any processing necessary to abide by the obligations set out therein.

Does the applicable law in Croatia allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

When considering this issue, it is important to note that under the Croatian Employment Act the employer is due to provide any devices or means of work to the employee. Therefore, there is no legal basis to require any employee to use any private device for work. The employer only has one possible legal basis to process an employee's personal phone number (which, of course, constitutes personal data) is consent. It is important to note what was already mentioned about employee consent.

The use of personal devices generally constitutes a security risk, so it is questionable whether it meets the security requirements set out in the GDPR. The answer will largely depend on the types and quantities of personal data processed and the security measures they are able to effectively implement even when the employees are using their own devices.

Some employers have chosen to enact special work from home policies or rule books which warn employees of behaviors that present a risk and are unacceptable from a security standpoint, such as using public Wi-Fi networks.

Does the applicable law in Croatia allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

In principle, the transfer of personal data, including special categories of personal data, through telecommunications networks is permitted. The compliance of such transfers with the regulations on the protection of personal data will depend on the means of transmission, storage and processing of such data. It is the responsibility of the data controller to make sure all of the hardware and software solutions they use in their business to process personal data are compliant by selecting only those devices, programs, methods, and services with a security level appropriate to the type and amount of personal data that is processed. Although the Agency for Personal Data Protection did not comment on specific requirements, regulators from other countries pointed out that, for example, ordinary e-mail communication is not considered sufficiently protected for the purposes of personal data security.

Does the applicable law in Slovenia allow and under what conditions does it allow processing of geolocation data?

In Croatia geolocation data can be processed like all other personal data in accordance with the provisions of the GDPR, when there is an appropriate legal basis

for the processing and the processing meets all the requirements of regularity and legality set out in the GDPR.

Due to the situation caused by the COVID-19 epidemic, the Government of the Republic of Croatia has proposed amendments to the Electronic Communications Act which would allow massive monitoring of location data originating from citizens' devices in cases of disasters and epidemics. The amendments have not yet been voted on and have encountered resistance from opposition members in the Croatian Parliament. At this point, therefore, the processing of geolocation data related to the COVID-19 disease epidemic cannot be discussed, but the processing of such data can only be assessed under general GDPR rules.

As the Council of Europe noted in a statement on the protection of personal data in the context of COVID-19, the development of such supervisory solutions should be based on a data protection impact assessment, and the processing should be designed in a way which minimally infringes the fundamental rights and freedoms of individuals.

KOSOVO

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Kosovo.

Does the applicable law in Kosovo allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

Health personal data are considered as sensitive personal data (Article 3, paragraph 1, sub-paragraph 1.5) according to the Law on Protection of Personal Data (Law on PPD), and as such, in principle, processing such data is prohibited (Article 8 (1)). However, exceptions exist in cases where:

1. processing is done for reasons of protecting substantial public interest 2.7),
2. where processing is necessary for the purpose of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of professional secrecy pursuant to respective legislation, established rules by national competent bodies or by another person subjected to professional secrecy (2.8);

There are no legal provisions in our legislation mentioning specifically body temperature. However, Law on Safety and Health at Work No.04/L-161 (Law on SHW) imposes the duty on the employer to apply preventive measures such as (but not limited to):

1. development of a comprehensive preventive policy regarding technology, work organizing, working conditions, social relations and impact of factors related to working environment;
2. giving priority to collective safety in relation to individual safety;

Moreover, the Law on PPD, allows restrictions on certain rights of the data subject , on cases where such restrictions are imposed in order to protect the fundamental rights and freedoms, and it is a necessary and proportionate measure to safeguard (Article 22): “other important objectives of general public interest of the Republic of Kosovo, in particular an important economic or financial interest of the Republic of Kosovo, including monetary, budgetary, taxation matters, public health and social security” (paragraph 1, sub-paragraph 1.5).

Based on legal provisions above, it can be concluded that there is an obligation of the

employee to inform the employer on a COVID19 infection occurrence. Namely, the Law on SHW makes responsible every employee to take care of his/her own safety and health at work, as well as that of other employees (Article 21(1)). In this line, the employee is under duty to: "notify immediately employer, the individual in charge of safety and health at work issues and employees' representatives, about any situation at work, for which he/she has a reasonable motive to assess as serious and immediate risk for safety and health at work;" (Article 21, paragraph 2, sub-paragraph 2.4)

Does the applicable law in Kosovo allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

The Law on Labor, No. 03/L-212, does not mention change of workstation/location (such as work from home). It only provides for temporary reassignment (Article 18), without the consent of the employee, which only mentions temporary reassignment (on specific circumstances) on work that requires lower professional qualification from the ones the employee possess (paragraph 1).

However, subject to employees' consent for work from home the legal framework provides for such an explicit measure in another piece of legislation: General Collective Agreement in Kosovo, which outlines a set of general applicable regulative norms that are fully recognized, and even authorized by the Labor Law. Since call forwarding implicates disclosure of certain personal data, the measures encompassed in the Law on PPD apply. Namely, the employer must apply appropriate technical and organisational measures, taking into consideration "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons" (Article 23 (1)). Such measures include: pseudonymization and encryption of personal data (Article 31, paragraph 1, sub-paragraph 1.1.); the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services (1.2.); the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (1.3.); a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing (1.4).

Does the applicable law in your jurisdiction allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

Online communication between the provider and the client in principle is allowed, however it should be based on basic principles on processing of personal data (principle of lawfulness, justice and transparency; principle of limitation of purpose; principle of data minimization; principle of accuracy; principle of storage limit; principle of integrity and confidentiality; principle of accountability) . The controller may refuse to act on the request of a data subject, when it is demonstrated that it cannot, and it is not able to identify the data subject (Article 11 (2) of the Law on

PPD).

As mentioned above, special categories of personal data can be processed only in very limiting situations. However, such restrictions and limitations will not apply in cases where Article 8 (2) of the Law on PPD):

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the relevant legislation in force provide that the prohibition may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by the relevant legislation in force or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relate solely to their members or data subjects who have regular contact with it in connection with its purposes and that the personal data are not disclosed without the consent of the data subjects;
5. if the data subject has made them public without limiting their use in an evidenced or clear manner;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of relevant legislation;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of professional secrecy pursuant to respective legislation, established rules by national competent bodies or by another person subjected to professional secrecy;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of relevant legislation;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The special categories of personal data are allowed to be processed as above, where the processing is proportional to the aim/objective the processing is trying to reach, and is performed in compliance with specific measures (technical measures; pseudonymization, data minimisation, professional confidentiality) for protection of special personal data (Article 8 (3)).

In cases where personal data are transferred to another country or to an international organization, the data subject is entitled to be informed in safeguard measures in connection to the transfer (Article 14 (2)).

Does the applicable law in Kosovo allow and under what conditions does it allow processing of geolocation data?

The Law on PPD allows for processing of geolocation data ("location data" in the law). To be more precise, location data are included in the category of personal data (Article 3, paragraph 1, sub-paragraph 1.1), and in this regard limitation on processing such data are the same ones as those imposed on other personal data (Article 5), namely:

1. if the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. if processing is necessary for the performance of a contract to which the data subject is a contracting party or in order to take steps at the request of the data subject prior to entering into a contract;
3. if processing is necessary for compliance with a legal obligation to which the controller is subjected;
4. if processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to the processing carried out by public authorities in the performance of their tasks.

If the processing is carried out for a purpose not mentioned above or based on the data subject's consent or based on a legal obligation of another legislation, then in order to assess the legality of such processing, the following will be taken into account (Article 5 (2)):

1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

3. the nature of the personal data, in particular if special categories of personal data are processed, or if personal data related to criminal convictions and offences are processed;
4. possible consequences of the intended further processing for data subjects;
5. the existence of appropriate safeguards, which may include encryption or anonymization.

CONTACT: info@adriala.com | www.adriala.com
Albania | Bosnia & Herzegovina (Banja Luka & Sarajevo) | Bulgaria | Croatia | Kosovo | Montenegro | North Macedonia | Serbia | Slovenia

NORTH MACEDONIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in North Macedonia.

Does the applicable law in North Macedonia allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID- 19 infection occurrence?

It should be noted that the Law on Personal Data Protection is by no means an obstacle to the implementation of measures to protection of public health, but nevertheless some recommendations should be taken into account.

Coronavirus prevention measures applied by state institutions, private companies and organizations may include the processing of personal data such as name, address, job, travel data, including specific categories of personal data such as data related to human health.

It is considered that the processing of personal data is legal if it is carried out for matters of public interest in the field of public health, such as protection against serious cross-border health threats, which include measures to protect the rights of personal data subjects, in particular protection of business secret.

It is also permissible to process data related to human health even when the person is not physically or legally able to give his consent, especially when it comes to emergency situations, in order to safeguard their essential and vital interests.

Controllers should provide clear, understandable and easily accessible information on the measures they take, as well as the purposes for collecting personal data and how long they will be kept.

Data security and confidentiality need to be ensured, especially when it comes to data related to human health.

It is important to note that the identities of persons affected by coronavirus should not be disclosed to third parties without a clear justification for such treatment.

Controllers are required to document decisions on the application of coronavirus measures involving the processing of personal data.

When it comes about the monitoring of bogy temperature the Employers have a legal obligation to protect the health of employees by justifying the collection of personal data in this particular circumstance for this purpose. For the use of even more stringent measures, such as submitting a questionnaire to employees and visitors

that should be filled in with this data, there should be serious justification only if necessary and proportionate and based on risk assessment.

Employers may require employees to inform them if they have been diagnosed with coronavirus so that appropriate action can be taken. However, any data related to health which is collected and processed should be justified and limited to what is necessary to achieve the objective of implementing health and safety measures. Following the directions of public health authorities and bodies, personal data may be disclosed for the public interest, with a view to protecting against a serious threat to public health.

In respect whether the employer should inform other employees that certain employees is infected by COVID-19, this should generally be avoided in the interests of confidentiality of the employee's personal data. For example, an employer may inform employees that there is or is suspected of having a coronavirus infection in the organization and require employees to work from home so that the person affected by the virus will not be named. However, disclosure of this information to public health authorities may be necessary to further carry out their functions.

Does the applicable law in North Macedonia allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

Article 153 of the Law on labor relations provides that in cases when human life and health, or the employer's assets are at risk, the type or place of carrying out the work, defined by the employment contract, may be temporarily changed even without employee's consent, but only within the duration of such state of affairs. In such a case, the employer may stipulate that the availability of a particular worker by telephone is strictly necessary for the performance of his / her tasks (e.g. for the purpose of working with clients) and should be provided with suitable working means (e.g. a business telephone).

We don't see any obstacle that the employee can make available his or her work resources to the employers such as call forwarding to his / her mobile phone, but explicitly consent to this should be in place or such consent may already exist in the employment contract.

Does the applicable law in North Macedonia allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

The new Law on personal data protection introduced in February 2020 is harmonized with the European legislation in the field of personal data protection, as follows: Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of personal data and for cancelation of Directive 95/46 / EC (General Data Protection Regulation) CELEX No. 32016R0679.

Online communication between the provider and the Client is not forbidden. Individuals can be linked to online identifiers, provided by their devices, applications, tools and protocols, such as IP addresses, identifiers called Cookies, or other identifiers and leave traces that combined with unique identifiers and others information obtained from the servers can be used to create the profiles of individuals and their identification.

That' why is important and the Operators are required to take appropriate technical and organizational measures in order to adequately manage the security risks of networks and services. In view of technical progress, these measures should ensure a level of safety appropriate to the risk involved. Operators of public electronic communications networks should take all appropriate steps to ensure the integrity of their networks and, at the same time, the continuity of the services they provide.

In cases where there is no compliance decision issued by the relevant body of the Directorate for protection of personal data, for reasons of public interest, the law may impose a restriction on the transfer of particular categories of personal data to a third country or to an international organization.

Does the applicable law in North Macedonia allow and under what conditions does it allow processing of geolocation data?

Location data that is not data referred to communication traffic related to subscribers or users of public electronic communication networks or public electronic communication services can be processed only in case of anonymity or on the basis of previously obtained consent of the subscriber or services user, to the extent and for the duration required to provide value-added services. The Operator shall, prior to obtaining the consent, be obliged to inform the Subscriber or the Service user on the type of location data to be processed, the purpose and the duration of the processing, and on the cases where such data shall be provided to third parties for the purpose of providing value added services. The subscriber or service user must, at all times, be given the opportunity to withdraw his/her consent to the processing of location data.

The Subscriber or Service user must be provided with the opportunity to, in a simple and free manner, temporarily refuse the processing of location data, for any connection on the public electronic communications network or for any communications transmission. The access to the processing of location data is permitted only to authorized persons of the operator of public electronic communications networks or public electronic communication services, or to third parties authorized to provide the value added services and must be limited to what is necessary to provide the value added service.

MONTENEGRO

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Montenegro.

Does the applicable law in Montenegro allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

Pursuant to the provisions of the Labor Law, employers are generally not entitled to process and collect health data of their employees, such as body temperature or other coronavirus symptoms. Such data is considered as one of the special categories of personal data and the applicable Personal Data Protection Law recognizes special restrictions on the processing of such personal data.

Even though the applicable Labor Law and Personal Data Protection Law do not provide for the possibility of implementation of the measures such as measurement of body temperature in the workplace by the employer, the obligation of the employee to inform the employer of an infectious disease may derive from certain measures applicable to health and safety at work. Namely, pursuant to the Article 18 of the Labor Law, the employee's is obliged to respect regulations for safety and health at work and perform work carefully while protecting own life and health, as well as life and health of others. Furthermore, Article 35 of the Law on Safety and Health at Work provides that the employer is obliged to immediately notify the employer, either in writing or verbally, or through employees' representatives, on any irregularities, defects, damages, dangers or other occurrence that could endanger his or her health or the safety and health of other employees, otherwise, failure to do so, would result in a misdemeanor offence by the employee. Since the respective employee may infect his co-workers with whom he was in contact, his obligation to inform his employer of a COVID-19 infection occurrence may arise from his obligation to protect his life, as well as life and health of the others. Certainly, this possible obligation of the employee would depend of the type and organization of the work and other relevant circumstances.

If the employer becomes aware that employee has COVID-19, either directly from the employee or otherwise, the employer shall threat such an information as personal data of that employee and is not allowed to disclose such information to any third parties, unless in the manner and under conditions set forth in the applicable regulations.

It is important to emphasize that Personal Data Protection Law generally provides that personal data may be used only subject to the provided consent of the person to which such data refers too. However, the Personal Data Protection Law provides legal basis for the use of personal data without the consent of the data subject and sets

forth several exceptions to this rule. Namely, Article 10 clause 2 and 4 of the Personal Data Protection Law defines that the processing of personal data may be performed without consent of the data subject if such processing is considered necessary to protect life and other vital interests of a data subject who is unable to personally consent to such a processing, and if it is necessary for the performance of activities of public interests. Furthermore, Article 13 of the Personal Data Protection Law, provides that special categories of personal data, such as health data information, may be processed without the express consent of the data subject if such use is necessary for the detection, prevention and diagnosis of diseases and treatment of persons, as well as for management of health services, if personal data are processed by a healthcare professional or another person who has an obligation of secrecy and where such processing is necessary for the protection of life or other vital interests of the data subject or of another person who has secrecy obligation.

These provisions quite broadly set forth the exceptions under which personal data may be used without the consent of data subject and hence, leave room for different interpretation. As a good example of such an interpretation, we can elaborate current situation due to the COVID-19 pandemic, where National Coordinating Body for Infectious Diseases of Montenegro requested an opinion of the Agency for Protection of Personal Data of Montenegro, as to whether they can publish personal data of the persons held in self-isolation (name and address) without their consent, on the basis of applicable legal provisions. In the Opinion no. 01-11-2261-2/20 as of 21 March 2020, the Agency found that such use and publishing of personal data was in line with above stated provisions of the Personal Data Protection Law and Law on Health Care which entitles citizens to be informed on the protection of their health in case of epidemics and other major disasters and accidents. This opinion speaks in favor of wide interpretation of both Personal Data Protection Law and other legal regulation, whereas in our opinion, use of personal data would be allowed in exceptional cases for use by public bodies, but does not allow public bodies to make such data public to all the citizens, as it was done in mentioned case. It is also questionable, whether the principles of necessity and proportionality would be found in such actions of the competent bodies of Montenegro, which are required for processing and use of personal data by third parties, including state and stated bodies.

Does the applicable law in Montenegro allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

Among other measures of protection from infectious diseases, all employers in Montenegro were instructed to consider and enable their employees to work from home. Work from home is also foreseen by the Montenegrin Labor Law.

In case that the employee does not have a business, telephone provided by the employer, the calls can be forwarded to the employee’s personal mobile device. The option of call forwarding is prescribed by the Articles 158 of the Electronic Communications Law of Montenegro. Although there is no specific provision

stipulates that is necessary to have a consent of the owner of the phone number to which calls are forwarded, we believe that an employee must give a consent for work calls forwarding to his private mobile device. This particularly bearing in mind that, pursuant to the Article 158 of the Electronic Communications Law, the operators shall provide the costumers with the possibility of barring of automatic call forwarding by a third party towards their terminal devices.

Does the applicable law in Montenegro allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

Montenegrin Personal Data Protection Law does not regulate in more detail means of communication through which personal data are transferred between the provider and the client, hence, we deem that such a transfer may be done even through telecommunication networks or similar. However, since the controller has to have either a consent of the data subject for the use of its data, or other legal basis for the use of such data, telecommunication networks transfer may pose a problem in case where the data subject needs to provide its consent, considering that securing the proof that such a consent was actually granted is rather complicated. Namely, according to Article 9 of the Personal Data Protection Law, the consent shall either be given in written form, or orally on the record.

In any case, whether the consent is or is not required, the data controller is obliged in accordance with Article 20 and 21 of the Personal Data Protection Law, to properly inform the data subject on the use of its personal data, and provide the data subject, with information on, inter alia, the name of the controller, use of its personal data and purpose of its use.

During the processing, i.e. use of personal data, regardless of the means of transfer and use, the data controller is obliged to implement technical, personnel and organizational measures to protect personal data against loss, destruction, unauthorized access, alteration, publishing and abuse. If the processing of personal data is done electronically, the collector of the personal data is obliged to secure that the information system automatically records users of personal data, data processed, legal basis for the use of data, the time of logging out and logging in from the system and similar.

Does the applicable law in Montenegro allow and under what conditions does it allow processing of geolocation data?

Electronic Communication Law of Montenegro regulates use of the personal data related to the use of telecommunication networks between the operator of electronic communication services and the client (customer). Article 173 of the Electronic Communication Law regulates that confidentiality of communication shall apply to, inter alia, geolocations, but that such data may be exceptionally used without the consent of the client, if such use is necessary, appropriate and

commensurate with national security interests, protection of the life and health of persons and property, and similar. In accordance with Article 175 of the Electronic Communication Law, the operator is required to delete or modify processed and stored traffic data related to its users, in such a way that they cannot be associated with a user when such data are no longer needed to transmit the communication and there is no obligation to withhold such data. However, according to Article 181 of the Electronic Communication Law, operators of electronic communication services, are authorized to withhold data on the geolocation and may provide such data to competent state bodies in case prescribed by the Electronic Communication Law, such as for the protection of national security interests and protection of life and health of the people. States bodies intending to use this data, must officially request them and, inter alia, specify the category of personal data, purpose of such a request, the legal basis for using and provision of the data for their use.

The basic principle regarding the processing and use of personal data by third parties envisaged in the Personal Data Protection Law, is that data processing is permitted only for the purposes for which it was intended and only to the extent necessary for such use. In cases which were accessed in practice by the Agency for the Protection of Personal Data of Montenegro, the Agency found that such use of data's pertaining to telecommunication networks is allowed without the consent of the client (customer) but must meet requirements of necessity and proportionality to the purpose of use of such data, even allowing operators to decline the request of public bodies.

As explained under item above, whatever the legal basis, the data controller is obliged to properly inform the data subject on the use of its personal data, and provide the data subject, with information on, inter alia, the name of the controller, use of its personal data and purpose of its use, in accordance with Article 20 and 21 of the Personal Data Protection Law.

SERBIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Serbia.

Does the applicable law in Serbia allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

As with all jurisdictions implementing GDPR, health data of employees fall to the special category of data, the processing of which is forbidden, unless falling within cases specifically designated under the law.

On April 1, 2020, Serbian Commissioner for Personal Data Protection came out with a statement on data processing during the state of emergency, pointing that there are no obstacles on processing health data when based on regulations in force, including acts adopted by competent state authorities during the state of emergency, where such processing must be carried out within the authorization limits and in line with all processing principles from the law.

On April 2, 2020, the Commissioner issued a statement welcoming the joint statement of the chair of the Committee of Convention 108 and of the Data Protection Commissioner of the Council of Europe on data protection during COVID-19 pandemics, pointing to some parts of the statement, including the one where the employers will probably be in the situation to process sensitive data, including health data. In that respect, the employers should only process data necessary for identification of potentially sick employees, fully in line with the principles of necessity, proportionality and responsibility. The risks to rights and basic freedoms of employees, especially as to the right of privacy, posed by such processing, should be minimized as much as possible. If the employer is requested to reveal employees' health data to state authorities, there must be a valid legal basis thereto. Upon ending of the state of emergency, the employers must get back to the ordinary regime of data processing, including permanent deletion of processed health data.

Concerning monitoring of body temperature, in its statement of April 1, the Commissioner pointed that processing of data regarding symptoms of potential COVID-19 infection of employees, candidates and other persons entering the business premises of the employer, could be allowed under the acts of competent authorities relating to combating the actual pandemics, but in line with data processing principles.

In that respect, the Government of Serbia issued a Decree on Organization of Work of Employers during the State of Emergency of March 16, 2020. The employers are to

organize remote work for all jobs where such work is feasible. Otherwise, the work should be organized (i) in shifts, in order to minimize the number of employees being simultaneously in one premise, (ii) all business meetings should be held remotely, and (iii) domestic and international business trips should be delayed. Also, employers are to provide all general, special and extraordinary measures regarding hygiene security of premises and persons in line with the Law on Protection of the Population from Infectious Diseases, for the purposes of ensuring employees' protection and health. However, it is unclear how would this actually operate, since, under the Law, powers and duties are generally vested to medical workers.

Under the Labor Law, the employer is to provide the employee with working conditions and to organize the work for the purposes of work safety and health, in line with this Law and other regulations. When it comes to health and safety at work, the employer is to hire the occupational health service. Also, the employee is obliged to inform the employer on any type of potential danger to life and health and risk of material damage.

As one of the exemptions from the prohibition on processing of health data, Serbian Law on Personal Data Protection exceptionally allows processing necessary for meeting obligations and applying of prescribed authorities of the controller or data subjects, in the field of labor, social insurance and social security, if such processing has been set under the law or collective agreement which sets for application of appropriate protection measures for basic rights, freedoms and interests of data subjects.

Digesting all above, the exceptionality of the situation seems to allow for processing of health data, but permissibility of such processing would have to be judged on case-by-case basis, with full respect of the provisions of the Law on Personal Data Protection. Therefore, potential input would concern the type and nature of the work, risks to health and safety of the employees etc. The processing would be more justified for those employees working from the office/business premises, than for those working remotely.

Temperature monitoring could be justified under the provisions of the Government Decree, however, it is advised to previously consult and get some feedback from the occupational health service and medical workers.

The reporting duty of the employee on COVID -19 infection occurrence would stem from the duties of the employee from the Labor Law. In order to be on the safe side, it is advisable for the employers to come out with a regulation or other bylaw or decision which would specifically tackle this issue. Also, all information obtained in such way fall to the processing duties under the Law on Personal Data Protection.

Does the applicable law in Serbia allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

Call forwarding to employee's personal mobile devices would be allowed only if there is legal basis set under the Law. Potential basis would include (i) consent of the data subject i.e. employee, (ii) if it is necessary for the employer completing his duties from the employment contract and, (iii) if it is necessary for completing legitimate interests of the controller.

In the light of the explained COVID-19 related measures, employers are required to organize remote work. If an explicit consent to call forwarding of the employee does not exist, and in the justifiable absence of any company mobile devices provided to employees working remotely, employer could forward calls to employees' personal devices if it is necessary for completing his duties under the employment contract. In line with the processing principles, such necessity would exist, inter alia, if the nature and type of the job position is such that the employee needs to communicate with partners, contractors or customers of the company, in order to complete his working duties. Calling upon legitimate interests of the company should be avoided as grounds for call forwarding, since justifying such processing on these grounds is the least feasible one.

Does the applicable law in Serbia allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

The relation between the provider and the client (user) is regulated under the Law on Electronic Communications. Under the Law, a written contract is required, which is to include provisions on personal data processing, during and after the contract ends. Therefore, transfer of data would have to be regulated under the contract between the provider and the client. Concerning communication flow data, the provider is further required to erase or make the data subject unrecognizable when such data are no longer required, save for situations set under the Law. In case of communication flow data necessary for making an invoice, which may be processed until the expiration of the legal deadline for making reclamations or for collection, before beginning the processing, the provider is to inform the client on the type of data processed as well as on the duration of such processing. In case of communication flow data used for advertising and sale of services or for providing value added services, the information has to be provided before obtaining the consent of the client.

The Law on Electronic Communications does not specifically regulate transfer of health data of the clients, nor such data fall within data required to be kept by the provider as under the Law. Therefore, rules of the Law on Personal Data Protection would apply. The Law requires application of technical, organizational and personnel measures in order to protect data processing. The Law mentions pseudonymization and encryption as one of the methods available in protecting, inter alia, the transfer of data. The provider is free to use other tools which provide adequate protection. For now, the Commissioner did not issue any instructions as to what is or could be deemed as adequate and/or appropriate telecommunication method of transfer. As

to grounds for processing of health data, please refer to explanations hereinabove.

Does the applicable law in Serbia allow and under what conditions does it allow processing of geo-location data?

In paraphrasing the joint statement, the Commissioner stated that processing of geo-location data for a larger number of subjects may be done only if, and on the basis of valid evidence, it could contribute to ending the spread of the pandemics. The processing should minimize the risk for privacy right, respectively it should be opted for the processing action which is the least aggressive to the accomplishment of the privacy right. These statements are clearly directing to strict compliance with the processing principles, such as principles of proportionality and legality.

The processing of geo-location data is becoming an important issue due to many employees working remotely due to COVID-19. The Government Decree points that the employer is to keep records on employees working remotely. In the absence of employee's consent, employer could call upon necessity of such processing arising from the employment contract. With data processing principles in mind, such necessity would exist only if employee's location is of importance for completion of employment rights & obligations. In the absence of any further explanations by the competent authorities, record keeping from the Decree per se does not imply the right of the employer to track the location of the employee.

Providers of public communication networks and publicly available e-communication services are subject to rules on data processing from the Law on Electronic Communications. Processing of location data, which do not represent data on the communication flow, is done either (i) on the consent of the data subject or (ii) only when data subjects are made unrecognizable, to the extent and within the time necessary for providing the services. Before obtaining the consent, the provider is to inform the user on the type of location data to be processed, the purpose and duration of the processing, as well as whether such data are going to be delivered to third persons, for the purposes of providing the services. Data subject has the right to recall its consent. The processing may be performed only by authorized personnel of the provider or by authorized personnel of a third party hired to provide the services, to the extent necessary for providing the service. The provider is also to provide for prevention measures as set under the Law. The Law also requires providers to keep the location data, but the access to such data is not allowed without the consent of the user (data subject), save for a limited time and on the basis of the decision of the court, if necessary for running the criminal proceedings or for the protection of Republic of Serbia.

SLOVENIA

An overview of the impact COVID 19 pandemic outbreak on the Data Protection matters in Slovenia.

We have prepared below a brief overview of certain opinions and positions of the Slovenian Information Commissioner (hereinafter: **IP**) regarding the processing and protection of personal data in the context of SARS-CoV-2 virus (COVID-19) outbreak, which we have summarized in the form of Q&A.

Does the applicable law in Slovenia allow and under what conditions does it allow processing of health data of employees, especially with respect to monitoring of body temperature of employees and possible obligation of the employee to inform the employer of a COVID-19 infection occurrence?

As a preliminary point, we emphasize that, in accordance with the provisions of the labor law legislation, employers are not normally entitled to process employees' health data, which includes data on the diagnosis, body temperature of employees, etc. Such data represents one of the special categories of personal data and GDPR provides in Article 9 that its processing of such data is prohibited unless any of the exceptions pursuant to Article 9 (2) GDPR are granted. According to the IP, at a time when we are experiencing the spread of COVID-19 infections and both individual and public health are threatened, special circumstances may require measures that may also interfere with the processing of special categories of personal data.

However, that is a question that needs to be answered primarily by the health care professionals, especially by an authorized occupational health-care professional. It can be discerned from the IP's opinions, that IP stems from the requirement that an appropriate person in the health profession must examine the necessity of individual measures aimed at achieving a specific goal. The IP also emphasizes that the necessity of individual measures should be examined in the light of concrete circumstances (what kind of work is involved, whether the work is conducted from home, what is the nature of the work, etc.).

Regarding the measurement and monitoring of employees' body temperature, the IP emphasizes the need to verify if there are other less invasive measures that may be even more effective in terms of actually preventing the spread of the infection and ensuring a smooth working process (such as, for example, as there were media reports about organizations organizing work in such a way that a certain group of employees work for a certain number of days, while others remain in domestic isolation (thus the possibility of infection is significantly reduced)). IP also expresses doubts about the need for continuous monitoring of employees. Furthermore, the IP considers that employers should, in the case they intend to introduce such measure, carry out a date protection impact assessment, which may also be specific, brief and concise. In any case, employees must be duly informed in accordance with Article 13

of the GDPR that such measurement or monitoring is being carried out.

The IP further considers that the justification of the employer's request that the employee is to notify the employer in the event of COVID - 19 infection depends on the type of work involved, how the employer arranged it and the nature of the work. Such obligation of an employee may be ordered by an individual company at the discretion of the competent institutions and the authorized person for occupational health-care (depending on the specific nature and organization of work) and taking into account the ZDR-1 (Employment Relationships Act) in connection with sectoral regulations and measures for ensuring health and safety at work. However, if the employer becomes aware of such information, the employer must ensure adequate protection and shall not be entitled to disseminate it without the appropriate legal basis. In principle, providing statistics (e.g., only information on the occurrence of an infection in a particular company, class, floor, etc.), without other information that enables the individual to be identifiable, is sufficient when dissemination of such information is necessary.

Does the applicable law in Slovenia allow and under what conditions does it allow call forwarding to the employees' personal mobile devices?

As a preliminary point, please note that the employer may also order work from home in accordance with Article 169 of the ZDR-1 (Employment Relationships Act), pursuant to which the employer may temporarily change the place of work during an emergency even without the employee's consent, but only for as long as such circumstances last. In such a case, the employer may decide that the availability of a particular employee by telephone is absolutely necessary for the performance of his / her duties (e.g. for the purpose of working with clients), but should provide the employee suitable working means (e.g. a business telephone).

The IP believes that the employee may also make available his or her work resources (such as call forwarding to his / her mobile phone) but must explicitly consent to this. The employer may, therefore, designate call forwarding to employees' private telephones, but must have the appropriate consent for such measure. Such consent may have already been given by the employee in the employment contract. In any case, the principle of data minimisation must be respected, which means that the telephone number should be used only to the extent absolutely necessary for the tasks of work from home. Upon termination of extraordinary circumstances, the employer may not further process or store the private number without the appropriate legal basis.

Does the applicable law in Slovenia allow and under what conditions does it allow online communication between the provider and the client and transfer of special categories of personal data through telecommunication networks?

Specific consent for online communication is not necessary, but it should be noted that individuals need to be properly informed, meaning that the data controller (i.e.

the service provider) should clearly and transparently communicate to the client regarding what personal data will be processed, for what purposes, what rights individuals have, etc., as required and provide by the Article 13 of the GDPR.

Personal data protection legislation does not prohibit the use of online tools and communication methods, but caution must be taken to ensure the security and confidentiality of data, especially when processing of special categories of personal data (e.g. health data) is involved. The data controller (i.e. the service provider) must verify that the individual tool enables confidentiality, in particular by enabling encrypted communication that prevents unauthorized persons from becoming familiar with the content of the communication. Details of the technical requirements for the transmission of special categories of personal data via telecommunications networks can be found at the following link: https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1448, regarding which we emphasize that regular e-mail as such does not provide special security.

Special consideration should also be given to the possibility of transfer of personal data to third countries, as many providers of such solutions come from the US. IP recommends checking if the solution provider is on the EU-US Certified Privacy Shield list (available at: https://www.privacyshield.gov/welcome).

Does the applicable law in Slovenia allow and under what conditions does it allow processing of geolocation data?

As a preliminary note, we emphasize that when it comes to the controller of personal data bound by the provisions of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No. 109/12, as amended; ZEKom-1), the special conditions and restrictions for the processing of geolocation data pursuant to Article 152 of ZEKom-1 must be respected. The aforementioned provision of ZEKom-1 applies for operators of electronic communications services.

In cases where the controller is not bound by the provisions of ZEKom-1 or the provisions of other special legislation, the decision on the legal basis for the processing of geolocation data must be taken by the data controller in light of the GDPR provisions, taking into account the specific context and purposes of processing such data and the risks to individuals' rights when processing their geolocation data. Such risk can be considerable when processing of geolocation data is conducted. In the absence of the express consent of the individual, the legitimate interests of the data controller could also be an appropriate legal basis. IP emphasizes that it is necessary to satisfy the test of weighting between the legitimate interest of the data controller on the one hand and the encroachment of the interests or fundamental rights and freedoms of the individual on the other. Such assessment must be carried out by the data controller.

In any case, the data controller must respect the basic principles of the processing of personal data, among others the principle of proportionality, pursuant to which the

data controller must choose the solutions that least affect the rights of individuals with regard to the processing of individuals' geolocations, taking into account the purpose pursued by the controller. IP considers that invasive measures, such as "tracking" individuals for a specific purpose (i.e. processing historical non-anonymized location data), can only be considered proportionate in exceptional circumstances and when strong safeguards for the rights of the individual are provided (i.e. that proportionality of processing with respect to duration and scope, data retention time limit and purpose limitation is ensured). Whatever the legal basis, the data subject must be properly informed in accordance with Articles 12, 13 and 14 of the GDPR.

CONTACT

ALBANIA - TASHKO PUSTINA

BOULEVARD DËSHMORËT E KOMBIT, TWIN TOWERS, COMMERCIAL CENTER 2ND FLOOR, 1019 TIRANA - ALBANIA

+355 4 238 91 90

+355 4 238 91 90

KEY CONTACT PERSONS:

Flonia Tashko: flonia.tashko@tashkopustina.com

Florian Hasko: florian.hasko@tashkopustina.com

BOSNIA AND HERZEGOVINA - BAROŠ, BIČAKČIĆ & PARTNERS, SARAJEVO

28 MARSALA TITA, 71000 SARAJEVO, BIH

+387 33 844 808

+387 33 844 809

KEY CONTACT PERSONS:

Nenad Baroš: nenad.baros@bblegal.ba

Feđa Bičakčić: fedja.bicakcic@bblegal.ba

BANJA LUKA

16 NIKOLE PASICA, 78000 BANJA LUKA, BIH

+387 51 961 780

+387 51 961 781

KEY CONTACT PERSON:

Predrag Baroš: predrag.baros@bblegal.ba

BULGARIA - SPASOV & BRATANOV LAWYERS´ PARTNERSHIP

29A SLAVYANSKA OFFICE CENTER "SLAVYANSKA", FLOOR 2, 1000 SOFIA, BULGARIA

+359 2 980 18 08

+359 2 980 25 10

KEY CONTACT PERSONS:

Georgi Spasov: georgi.spasov@sbn-law.com

Boyko Bratanov: boyko.bratanov@sbn-law.com

CROATIA - MADIRAZZA & PARTNERS ATTORNEYS AT LAW LLP

21 MASARYKOVA, 10000 ZAGREB, CROATIA

+385 1 48 77 280

+385 1 49 20 801

KEY CONTACT PERSONS:

Josip Madirazza: jmadirazza@madirazza.hr

Tin Težak: ttezak@madirazza.hr

KOSOVO - TASHKO PUSTINA

FEHMI AGANI, H. 79, K. 1, No. 1, 10000 PRISTINA, KOSOVO

+383 38 71 77 55

+383 38 71 77 55

KEY CONTACT PERSONS:

Gentian Gurra: gentian.gurra@tashkopustina.com

Floran Pustina: floran.pustina@tashkopustina.com

NORTH MACEDONIA - LAW FIRM KNEZOVIĆ & ASSOCIATES

10 KOSTA SAHOV St., 1000 SKOPJE, NORTH MACEDONIA

+389 2 322 06 80

+389 2 322 06 90

KEY CONTACT PERSON:

Dejan Knezović: dejan.knezovic@knezovic.com.mk

MONTENEGRO - PRELEVIĆ LAW FIRM

130 BULEVAR SV. PETRA CETINJSKOG KULA NCO/VII FLOOR, 81000 PODGORICA, MONTENEGRO

+382 20 510 506

+382 20 510 507

KEY CONTACT PERSON:

Dragan Prelević: dp@prelevic.com

SERBIA – BOPA BOJANOVIC PARTNERS

12 VLAJKOVICEVA, 11000 BELGRADE, SERBIA

+381 11 414 52 80

+381 11 414 52 89

KEY CONTACT PERSON:

Vladimir Bojanović: vladimir.bojanovic@bopa.rs

SLOVENIA - LAW FIRM KAVČIČ, BRAČUN & PARTNERS, O.P., D.O.O.

TRG REPUBLIKE 3, 1000 LJUBLJANA, SLOVENIA

+386 1 244 55 00

+386 1 244 55 01

KEY CONTACT PERSONS:

Matej Kavčič: matej.kavcic@kbp.si

Simon Bračun: simon.bracun@kbp.si

info@adriala.com
www.adriala.com