C/M/S/

Law . Tax

Coronavirus (COVID-19) and Privacy

Begin >

What to look for when restarting workplaces?

2020

Menu

Your key contacts in CEE & UK ▸

Bulgaria

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

Bulgaria has no COVID-19 specific data protection-related law or guidance. The Bulgarian parliament adopted the Act on the Measures and Actions during the State of Emergency, declared by a Resolution of the National Assembly of 13 March 2020 and for overcoming its consequences (the "**State of Emergency Act**"). However, the only provision related to processing personal data in the State of Emergency Act relates to data for mobile cell areas processed by mobile operators. At the request of officials from the Ministry of the Interior, such data must be immediately provided to them for the purposes of enforcing mandatory isolation or hospital treatment of infected persons who do not comply with the requirements for mandatory isolation or treatment.

The Bulgarian Labour Code provides for a general obligation on employers to secure occupational health and safety for employees. However, no specific instruction to employers or amendment to the Labour Code has been introduced to clarify data protection issues in light of the pandemic.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The Data Protection Authority in Bulgaria (*Комисия за защита на личните данни*, the "**DPA**") has not published any comprehensive guidance regarding processing personal data during the State of Emergency.

The DPA has issued just one statement (LINK) on the lawfulness of the Ministry of the Interior processing personal data by collecting declarations from citizens passing through checkpoints in regional cities. The declarations must contain the reason for travelling, i.e. work related, health related or returning home. The DPA explained that the data protection legislation allows the possibility to limit the scope of citizens' rights and freedoms pursuant to Article 23 of the GDPR, and in this case the measure imposed by the Ministry of the Interior is necessary and proportionate in view of safeguarding public health and the prevention of threats to public security.

Additionally, the DPA has published a link on its website (LINK) to the Guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak and the Guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak of the European Data Protection Board.

We are not aware of the imposition of penalties in respect of COVID-19 related data protection breaches. There have been penalties imposed in respect of COVID-19 breaches regarding breaking mandatory isolation, visiting parks (which was forbidden for a certain period) and not wearing protective masks.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

As is the case with any contagious disease, the health authorities and medical personnel are obliged to report all cases of COVID-19. However, no such legal obligation is imposed on employers regarding their employees.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

By an order of the Minister of Health (*министър на здравеопазването*) employers are obliged to introduce work from home arrangements for their employees, if the nature of the work allows it. The State of Emergency Act further provides the possibility for employers to assign home offices to their employees without their consent. The terms and conditions of assignment, fulfilment and control of work from home are determined by the employer. There are no official recommendations or requirements. Each employer decides and imposes its own cybersecurity measures.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

There is no local law or local regulatory guidance applicable to this. Therefore, the general GDPR principles apply i.e. the data will be retained for no longer than is necessary for the purposes of the processing.

6. Have any local digital technologies been developed or released in response to COVID-19?

A free mobile application, ViruSave, has been developed by Bulgarian IT specialists in response to COVID-19. Any citizen can download it and share his/her health status with the National Operative Headquarters, the health authorities and his/her personal doctor on a voluntary basis. The information is used for statistical purposes.

Croatia

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

Croatia has no specific COVID-19 data protection-related law. However, there is a general obligation on employers to secure health and safety in workplaces. Under the Labour Act, employers are obliged to protect the life, health and morals of employees and must, among other things, organise work in a manner that guarantees the protection of life and health of employees in accordance with special laws and other regulations, and in accordance with the nature of the job being performed. Further, the Act on Health and Safety at the Workplace states, among other things, that its main purpose is to systematically improve the health and safety of employees and to prevent work-related injuries, professional diseases and work related diseases.

In addition, under the Labour Act employees must notify their employers of illness or other circumstances which prevent them from, or essentially interfere with, their fulfilment of their obligations under their employment contract, or which endangers the life or health of persons with whom the employees come into contact during the performance of the employment contract.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The Croatian Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka*) issued a statement on 18 March on the processing of data concerning health in the context of COVID-19, which mainly deals with the processing of employees' data.

Key takeaways:

- The "main" applicable legal basis for processing is Article 6 (1) c) of the GDPR, where processing is necessary for compliance with a legal obligation to which the controller is subject, such as the aforementioned legal provisions of the Labour Act and the Act on Health and Safety at the Workplace. Alternatively, Article 6 (1) d) can be relied on, where processing is necessary to protect the vital interests of the data subject or of another individual person.
- Further, for processing data concerning health (as a special category of personal data for which specific requirements are prescribed), Article 9 (2) b) can be relied on, where the processing is necessary for carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment and social security and social protection law, insofar as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Not every personal data processing can be justified on the basis of the above provisions of the Labour Act and the Act on Health and Safety at the Workplace, and the main principles of the GDPR must still be respected (such as proportionality, necessity, and data minimisation), especially when processing data concerning health.

We are not aware of any notable cases or COVID-19 related breaches so far.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

The Croatian Institute of Public Health, Department of Occupational Health (*Hrvatski zavod za javno zdravstvo, Služba za medicinu rada*), noted in its instructions to employers and employees that if an employer suspects its employee has been infected with COVID-19 (e.g. an employee shows symptoms), an employer's health and safety expert or another responsible person must notify an authorised epidemiologist. Note that employees are also obliged to notify their employer's health and safety expert or another responsible person of any signs of (possible) COVID-19 infection so that employers can ensure necessary health-protection measures for other employees. Information on the results of the COVID-19 tests are further communicated to the government authorities by epidemiologists and other healthcare bodies.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

No specific recommendations or guidelines have been issued in this respect. However, companies should always be careful and ensure that appropriate security measures are in place for home working (e.g. secure remote access to emails, servers). This should also be aligned with the requirements for security in processing personal data envisaged by Article 32 of the GDPR.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

There is no specific local law or regulatory guidance on this matter. Here, the main principles of the GDPR still apply, especially the storage limitation principle, which is also included in Croatian Personal Data Protection Agency's existing guidance on the COVID-19 pandemic. Companies should not keep and process personal data longer than necessary for the purpose for which the data are processed. Generally, it is not expected that personal data will be needed subsequently/following the end of the extraordinary governmental measures for combating the COVID-19 pandemic. Each assessment should be made on a case-by-case basis, and the aim should be not to retain data longer than needed for a specific purpose. In addition to the GDPR principles, the Labour Act prescribes that employees' personal data must be erased or otherwise removed if there is no longer any basis for storing them.

6. Have any local digital technologies been developed or released in response to COVID-19?

Yes. Croatia has developed and released a digital assistant powered by artificial intelligence, with the purpose of advising people on how to diagnose and manage suspected COVID-19 infections. This digital assistant is called *Andrija* and can be activated on WhatsApp.

In addition, the Croatian Minister of the Interior recently announced that the Government is considering a voluntary contact tracing app. No further information is available at the moment and it is not yet known how the app will work. Additionally, certain amendments to the Electronic Communications Act have been proposed which should broaden the possibility of processing location data other than traffic data in special circumstances such as the COVID-19 pandemic.

Czech Republic

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

No COVID-19 specific data protection-related law is in place. Under the Czech Labour Code, employers have a general obligation to secure occupational health and safety for the individuals present at the workplace. Employers must: (i) create a safe and harmless working environment and working conditions through suitable organisation of occupational health and safety protection and by adopting measures to prevent risks; and (ii) continuously seek out dangerous factors and processes in the working environment and working conditions (i.e. carry out risk assessments), determine their causes and sources, and adopt measures to eliminate such risks.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The Czech data protection authority (*Úřad pro ochranu osobních údajů*, the "**DPA**") has not published any comprehensive guidance regarding processing (health) related personal data at the workplace. However, with regard to the COVID-19 pandemic, the DPA stated that employers must take appropriate measures to ensure compliance with their respective health and safety obligations and admitted the possibility of temperature screening.

The DPA has recently provided clarifications regarding the body temperature screening of employees and other individuals at the workplace. The DPA confirms that regarding the current situation and employers' health and safety obligations, such measure and subsequent data processing can be considered as a legitimate interest regarding employers fulfilling their obligations and exercising specific rights concerning data processing in the field of employment (a reference is made to Articles 6 (1) (f) and 9 (2) (b) of the GDPR). However, the DPA added that an employer has to take into account several elements (and scrutinise them continuously) to keep such measure proportionate, e.g. the nature of the workplace, number and concentration of employees at the workplace and the development of the pandemic. The DPA also stated that once the pandemic has passed, such processing is likely to be unjustified.

Regarding the above, employers should carry out a balancing test, data protection assessment and duly inform the affected persons of such processing of their personal data.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Yes, however these apply particularly to subjects in the health care sector. The Ministry of Health has issued a number of extraordinary measures subjecting healthcare providers, social care and homecare providers and other public health institutions to reporting data collected when testing for COVID-19 and other relevant healthcare data.

The following data must be reported to the Ministry of Health:

- all tests done on patients for the presence of virus SARS-CoV-2;
- prescribed personal data of the tested patients (name, surname, birth certificate number, date of birth, residency address, contact details);
- all results of the tested patients;
- intensive care capacity in terms of available extracorporeal membrane oxygenation beds, artificial lung ventilation (UPV) beds and other mandatory capacities; and
- the numbers healthcare professionals who are quarantined at any given time for suspicion or a positive diagnosis of COVID-19.

Additionally, an obligation for banks and mobile network operators to share certain personal data is set out in the programme called "Smart Quarantine" (please see below).

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

No. The Government issued a crisis measure which recommends that employers resort to remote working options for the duration of the state of emergency, however the recommendation does not contain any cyber security recommendations.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

The principle of storage limitation applies. COVID-19 related personal data should be kept only for as long as necessary for the purposes for which the personal data are processed.

6. Have any local digital technologies been developed or released in response to COVID-19?

The Ministry of Health launched a programme called "Smart Quarantine" which is supposed to track and isolate the contacts of people with SARS-CoV-2 by tracing their movements via their SIM cards and their credit/debit cards, subject to the consent of patients who test positive. Private sector companies such as banks and mobile network operators are obliged to cooperate with the public authorities and share the relevant personal data with them.

As part of the Smart Quarantine programme, a tracking app for smartphones has been developed which uses Bluetooth to track the user's movements to follow whether they have been in proximity of someone who later tested positive for COVID-19. This app does not track and collect user's location, but only anonymously detects which other users of the app the person has come into close contact with. Nevertheless, certain personal data are processed (e.g. phone numbers) with the data controller being the Czech Ministry of Health.

Furthermore, one of the largest Czech IT companies, Seznam (operator of the internet browser seznam.cz) provides a function in their map app for smartphones, equivalent to the Google maps app, which calculates the possibility of being exposed to the virus by taking into account location data provided by healthy as well as by infected people. The provision of data is on a strictly voluntary basis.

Hungary

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

On 18 June 2020, Hungary lifted its state of emergency, and decrees passed to tackle the COVID-19 crisis, such as Government Decree No. 47/2020. (III. 18.), are no longer in effect. Companies may still consider necessary and reasonable measures to check the health of employees, but they must assess the legal basis with a view to Articles 6 and 9 of the GDPR.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

Hungary's Data Protection Authority (*Nemzeti Adatvédelmi és Információszabadság Hatóság*, the "**NAIH**") has issued two documents regarding the processing of personal data vis-à-vis procedures for preventing the spread of COVID-19:

- A general guidance to organisations on 10 March 2020. The NAIH emphasised that it had formulated its opinion with a view to the situation of the pandemic in Hungary on that date.
- An individual statement for companies on 28 April 2020.

Key takeaways:

- Organisations can introduce mandatory diagnostics and screenings but only with the assistance or supervision of healthcare professionals or nurses/ human resources employees under their professional responsibility.
- Employers must prepare a risk assessment as to whether data processing (e.g. temperature checking) it is absolutely necessary for a certain position (e.g. customer-facing employees who are particularly affected by potential exposure).
- The legal basis of the data processing is Article 6 (1) f) (legitimate interests) and Article 9 (2) h) (preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, under the responsibility of a professional subject to professional secrecy) of the GDPR.

To reduce privacy risks, organisations must prepare a data protection notice, a legitimate interest-balancing test (*érdekmérlegelési teszt*) and a data protection risk assessment.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Until the end of the state of emergency (*veszélyhelyzet*), organisations must provide information on request to the COVID-19 Operative Authority (*Operatív Törzs*) established by the Government to: (i) prevent, analyse and fight the spread of COVID-19; and (ii) organise the defence of the governmental institutions. The Operative Authority also has the right to access the identification, address, contact and health data of those people who are infected, or suspected of being infected, with COVID-19, together with the same data of their contacts.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

- The Hungarian Cybersecurity Institute (*Nemzeti Kibervédelmi Intézet*) published a Warning on Spam emails related to the COVID-19 pandemic.
- The Hungarian Cybersecurity Institute published Recommendation on Secure Home Office.
- The Ministry for Information and Technology also published a Warning that false information about tenders is being spread concerning development policy measures regarding COVID-19.
- The Hungarian BAR Association issued a resolution on permitted electronic communications equipment for remote client identification. The use of Zoom is not allowed by lawyers.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

General data retention rules shall apply. It may be necessary for employers to keep certain personal data, if they took certain measures on the basis of health data (e.g. did not permit someone to enter their premises because he/she had a fever, or someone infected other employees with COVID-19), or the data may be necessary for the establishment, exercise or defence of legal claims.

6. Have any local digital technologies been developed or released in response to COVID-19?

Based on a person's voluntary consent, the competent health authority (*járványügyi hatóság*) may order the installation of a software app to monitor the individual's compliance with the home quarantine rules. The app tracks the person's movement and may transfer his/her location data, image and (COVID-19 related) health data to the police and the competent health authority. VirusContact is a mobile app, currently under development. Its purpose is to send an anonymous notification to individuals if they were near to an infected person in the preceding 14 days regarding when, where, and how far. "Life Saver" (*ÉletMentő*) is an application from the National Ambulance Service (*Országos Mentőszolgálat*) and Vodafone Foundation, which sends push notifications to its users on COVID-19 related information.

Poland

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

In Poland the legal landscape related to the COVID-19 crisis is mainly regulated in the Act of 2 March 2020 on Specific Solutions related to the Prevention, Combating and Eradication of COVID-19, other Infectious Diseases and Crisis Situations Caused by Them ("COVID-19 Act") and acts amending it.

Data protection aspects are not extensively covered in the COVID-19 Act and the guidelines of the Polish Data Protection Authority (*Prezes Urzędu Ochrony Danych Osobowych*, "**UODO**") and Chief Sanitary Inspector (*Główny Inspektor Sanitarny*, "**GIS**") play a role in this field.

The COVID-19 Act introduced the possibility for the Chief Sanitary Inspector to issue binding recommendations, in particular to employers, on taking certain preventive or control measures. Importantly, these recommendations can serve as a legal basis for processing personal data. The UODO stressed this aspect in its latest guidance, stating that temperature checking or processing other health data, e.g. in the form of health questionnaire, should be based on GIS's recommendations. Notably, the UODO excluded consent as a legal basis for processing employees' data about health in the context of the COVID-19 crisis.

The UODO has also published guidance on remote working and remote education, please see 4 point below for more details.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The UODO has not issued any decisions concerning data protection during the COVID-19 pandemic yet which are publicly available.

The UODO has stressed that data protection law does not prevent employers from processing the data, including health data, of employees or visitors during the COVID-19 pandemic. However, the GDPR applies and employers must secure a valid legal basis for processing. As mentioned above, recommendations of the Chief Sanitary Inspector may serve as such a legal basis.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Based on pre-COVID-19 rules, any person residing in Poland is obliged to provide relevant institutions, such as the State Sanitary Inspectorate, with information necessary for the epidemiological surveillance and prevention and control of infections and communicable diseases. This this is an obligation on each employee and applies to COVID-19.

In addition, the COVID-19 Act introduced an obligation for telecommunications operators to make available to the Minister of Digital Affairs:

- data on the location, for the preceding 14 days, of the telecommunications equipment (such as smartphone) of an end user suffering from the COVID-19 infectious disease or under quarantine;
- anonymised data on the location of the terminal equipment of end users.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

The COVID-19 Act has introduced a possibility for employers to order employees to work remotely to prevent COVID-19. However, no rules concerning cybersecurity were specified.

Some general guidance can be found in the UODO's advice (available only in Polish) on security regarding the use of devices, email, networks and the cloud in the context of remote working. The UODO also indicated that employers must ensure that paper documents used remotely should be limited to what is necessary and that any personal data included in them should be processed securely. According to UODO, employers must also introduce a procedure for destroying paper documents.

In addition, the UODO issued guidance for schools relating to remote education, indicating e.g. that when using applications for remote education, it should be verified whether sharing personal data is necessary and if yes, they should be minimised or pseudonyms should be used instead of real names.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

No particular local law or guidance has been issued in this respect.

6. Have any local digital technologies been developed or released in response to COVID-19?

The COVID-19 Act introduced an obligation (with a few exceptions) for persons on quarantine to download and use an app made available by the Ministry of Digital Affairs called *Kwarantanna domowa*. The application uses geolocation and a facial recognition system and requires the person on quarantine taking pictures of themselves (*selfie*) at different times of the quarantine. The Minister of Digital Affairs is the controller of the personal data and users' personal data may be shared with, e.g. the police, voivodes, and Information System Centre for Health Protection. Pursuant to the Privacy Policy, data collected during the use of the application will be stored for six years.

A second app, called *ProteGO Safe*, is currently being developed. It is a contact tracing application, based on Bluetooth technology, that aims to prevent the spread of COVID-19. It is not regulated at a statutory level yet. Based on governmental declarations, its use will be voluntary.

Romania

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

No specific COVID-19 data protection-related law has been adopted at the local level. Nevertheless, pursuant to Order No. 3577/2020 issued by the Ministry of Labour regarding health and safety measures to prevent COVID-19 spreading during the state of emergency, employees are legally obliged to accept that their body temperature is checked on entering the workplace.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

So far, the National Supervisory Authority For Personal Data Processing (*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*) has published on its website: (i) the legal grounds, as per GDPR, on the basis of which personal data concerning health can be processed; and (ii) a statement of the processing of personal data in the context of COVID-19, adopted by the European Data Protection Board at the following link: LINK. Therefore, there are no specific provisions/recommendations individualised for Romania, nor any COVID-19 related breaches of which we are aware.

With regard to other competent authorities such as the Ministry of Health or the Ministry of Labour, the focus of these authorities during the COVID-19 pandemic is to create a safe work environment by putting in place health and safety measures. The authorities do not seem to be particularly with how their measures could affect other areas of law, the most important being the data protection laws safeguarding individuals' personal data.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Yes. If an employee is confirmed as having COVID-19, companies are obliged to inform the Public Health Directorate (*Direcția de Sănătate Publică*) from the county where the activity is carried out, which will be followed by an epidemiological investigation. In addition, COVID-19 data may be requested at the border from persons entering Romania.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

During the state of emergency, teleworking or work from home may be decided upon with the employee's consent. In such case, the general requirements regarding health and safety at work must be observed.

The Information Technology and Cyber Security Service has issued a number of rules to be considered during the COVID-19 pandemic, such as: using only encrypted communication channels (SSL VPN, IPSec VPN), assessing possible security risks and informing the employees of them, appointing a person who provides remote support to employees in the event of technical or security errors, etc., which can be accessed here: LINK

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

As a rule, companies may maintain such measures for as long as necessary, e.g. until the COVID-19 pandemic has abated. However, if the measures have been implemented as per an obligation imposed by the current legislation regarding the prevention of COVID-19, these measures may be limited to the period during which the legislation remains in force, e.g. the obligation to check the body temperature of employees will apply until the state of emergency ends.

6. Have any local digital technologies been developed or released in response to COVID-19?

So far no such digital technologies have been developed at the local level or are available to public. There are several apps which are accessed by public authorities, e.g. a medical data management app used by the Ministry of Health. We also note that Code for Romania, a youth community which develops IT solutions for society, is currently working on several apps that are designed to inform the public of relevant information regarding the spread of COVID-19.

Russia

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

The Russian data protection authority (The Federal Service for Supervision of Communications, Information Technology and Mass Media, *Roskomnadzor*, the "**DPA**") has issued clarifications regarding data processing issues related to the use of thermal cameras. The DPA has acknowledged this information as special categories of personal data (health data), but has also stated that this data can be processed by employers on the basis of general rights under the Labour Code allowing employers to process health data to check the ability of an employee to perform his/her job. Regarding visitors to the controller, the DPA assumes that consent is given by the action, i.e. entering the premises.

No other clarifications have been issued so far. However, these clarifications might be extended so that employers are able to check the temperature and do COVID-19 tests on employees without additional consents.

Additionally, at the federal and regional levels (e.g. in Moscow), employers are obliged to check the temperature and prohibit employees entering premises who have a positive COVID-19 result. This is an additional confirmation that in the current circumstances, employers can process some additional information regarding health to prevent spread of COVID-19.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

Except for the clarifications by the DPA mentioned in question 1, there are no other cases.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Yes, if an employer detects that an employee has a positive COVID-19 test, it must inform the local authority (local division of the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing) upon its request of this fact and this person's contacts with other individuals.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

There are no general recommendations regarding cybersecurity issues, and all companies will decide themselves what the measures should be to protect confidentiality during remote working.

For the banking sector, the Russian Central Bank has issued general recommendations for banks to ensure stable transactions during the COVID-19 pandemic.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

No specific regulations. The general storage limitation principle should apply to COVID-19-related information.

6. Have any local digital technologies been developed or released in response to COVID-19?

Some regions of Russia (e.g. Moscow, the Moscow region and the Kemerovo region) have introduced or are going to introduce a system of digital passes allowing citizens to leave their homes for certain purposes, e.g. to visit a medical organisation, to go to work if the employer is allowed to operate. A pass is not necessary to go to the closest supermarket/pharmacy or walk a dog. The digital passes can be received online.

Digital passes can be checked by law-enforcement officers, who can check individuals who are outside. In the absence of a pass, a fine might be imposed.

In addition, in some regions (e.g. Moscow) traffic cameras are used to identify vehicle number plates and check whether a pass has been issued to a vehicle.

Furthermore, a system of monitoring individuals has been launched to check whether the quarantine regime (e.g. for those who have returned from abroad) is complied with and to identify contacts with other persons. In the event of a breach, the breaching person receives an SMS with a warning; this information might be transferred to law-enforcement agencies. The monitoring system is based on information regarding users' location from mobile operators. Despite several public complaints, the Ministry of Digital Development, Communications and Mass Media has announced that in its view, this system complies with all data protection laws.

Serbia

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

No COVID-19 specific data protection-related law is in place.

However, the Labour Law obliges the employer to provide employees with working conditions and organise work in a manner which provides an appropriate level of safety and protection at work. Additionally, the Law on Safety and Health at Work regulates the implementation and improvement of safety and health at work of persons who do work, as well as persons who are in the work environment, to prevent injuries at work, occupational diseases and diseases related to work. Thus, the employer's obligations could be used as appropriate legal grounds for processing such sensitive personal data.

Further, the Law on the Protection of the Population from Infectious Diseases could also be used as legal grounds for processing the above data. This law obliges all companies, including private entities, to take the necessary preventive measures adopted by the Government during a pandemic to stop the spread of the disease.

Nevertheless, in all of the above cases, the employer should choose the less intrusive measure, e.g. it cannot introduce blood testing if the result can be achieved through the less intrusive measures such as using health data questionnaires, measuring body temperature, etc.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The commissioner for information of Public Importance and Personal Data Protection, *Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti* (the "**Commissioner**") has published an announcement appealing to the media to refrain from publishing data on persons infected with the corona virus. There have been frequent cases of news reports about Serbian citizens who have been infected, with published information about those persons who make their identity public or identifiable. For more details, please refer to the following link: http://skr.rs/pBW

In addition, one remarkable example of a COVID-19 related breach is the situation where the headquarters for emergencies in Šid published on its media platforms the initials, workplace, age and residential street of the first person infected with the corona virus in this location, and thus fully revealed the identity of the infected person, a medical worker. According to the Law on Patients' Rights, which refers to the right to confidentiality of data on the patient health, data from medical documentation are particularly sensitive data. The unauthorised disclosure of such sensitive information is punishable. Medical data is also protected by the Law on Personal Data Protection, which is why the Commissioner initiated supervision. For more details, please refer to the following link: http://skr.rs/pB1

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Yes, however such provisions apply to subjects in health care sector i.e. to health care institutions, private practice, health care workers, etc.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

Yes, there are. Here are recommendations/announcements.

- The Regulatory Agency for Electronic Communications and Postal Services of the Republic of Serbia has issued recommendations and a warning regarding Zoom (it was not blacklisted, but the recommendation was on how to safely use the platform). For more details, please refer to the following link: https://www.cert.rs/en/obavestenja.html
- The Commissioner has warned citizens of possible fraud via social networks in the form of "offers for help" from strangers, which, for the sake of alleged assistance, ask for current account and credit card numbers, ID card number, Personal Identification Number and other personal data. The Commissioner further emphasised that citizens can directly contact the competent body or institution and to report such "offers". For more details please refer to the following link: http://skr.rs/pBq
- The Ministry of Education has warned schools that they are obliged to protect students from digital violence, i.e. that teachers should not ask students to send them videos/photos in order to prevent any kind of child abuse in cyberspace. This because no one can be sure that a teacher's email is protected from "intrusion" and then from abuse of such videos/photos. In addition, the Commissioner considers that the collection of contact data (telephone numbers, email addresses) for the purpose of uninterrupted distance learning, may represent an necessary processing of personal data, of course with all available data security measures being taken.

For more details, please refer to the following link: http://skr.rs/pBh

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

There are no specific regulations regarding processing COVID-19 related data, however a general rule can be applied to this matter: if the deadline for maintaining it is not prescribed by law, the controller is allowed to set an appropriate deadline, still the collected personal data should be kept only for as long as necessary for the purposes of processing.

6. Have any local digital technologies been developed or released in response to COVID-19?

No, there have not been any digital technologies released in response to COVID-19.

Slovakia

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

The Slovak Data Protection Office (*Úrad na ochranu osobných údajov Slovenskej republiky*) has issued a statement pursuant to which Article 9 (2) (i) of the GDPR (public interest in public health) represents the appropriate legal grounds for temperature measuring, subject to the existence of a relevant local law. The DPA considers the guidelines of the Public Health Authority (*Úrad verejného zdravotníctva Slovenskej republiky*) as the relevant local law. The guidelines provide guidance concerning temperature measuring at entrances to hospitals and industrial plants. Temperature measuring is also not ruled out in other places, but there are no official guidelines for controllers operating such other places.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

We are not aware of any cases where the Slovak Data Protection Office has decided on COVID 19 related breaches so far.

In most of its statements, the Slovak Data Protection Office has referred to the guidelines of EDPB.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

The guidelines of the Public Health Authority state who is obliged to share data relating to a suspicion or confirmation of COVID-19 infections with the government. The types of data are not specified and it can be assumed the authorities will specify the data they need. Typically, this concerns healthcare providers, emergency service providers, persons in charge at specified border crossings, persons in charge in facilities of resorts of defence, internal affairs and transport.

Private companies must **notify** the Public Health Authority and the Regional Public Health Authority without undue delay of **all relevant circumstances** for the prevention and spread of notifiable diseases and other work-related diseases, and provide them with information relevant to the epidemiological examination and disease assessment in the work performed. A direct obligation to **report a confirmed case** of COVID-19 to the authorities is imposed only upon the healthcare providers or a health care professional (i.e. not private companies in general). However, as the above "notification obligation" to relevant authorities is drafted in a rather general manner, as a best practice private entities may decide to liaise with the Public Health Authorities on the further steps which should be taken when learning relevant data about COVID-19.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

The National Security Authority has issued guidelines.

- For videoconference calls, only use known platforms with a good reputation (Zoom is not recommended).
- When working from home, employees should regularly communicate with their employers and with the colleague responsible for IT and cyber security. They should notify all suspicious events and circumstances (phishing emails, suspicious calls and SMSes, non-standard computer functioning, etc.).
- Infrastructure security must be a priority for employers, and they should provide employees with guidelines about working from home safely.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

According to the Slovak Data Protection Office, the measures should last only until the end of the exceptional situation (the state declared by the government).

6. Have any local digital technologies been developed or released in response to COVID-19?

Slovak volunteers and experts created the "stay healthy" (*ZostanZdravy*) app in a short time to help slow the spread of COVID-19.

If: (i) a user approaches a critical distance (50m) from another user who has tested positive for COVID-19; or (ii) someone with whom the user has come into contact within the distance of 50m in recent days has just tested positive, the application will send a warning message to the user. After that, it will be up to the user to decide whether he/she should get tested immediately or only after the first symptoms present. People can book a test through the app and will receive the results directly to the app through a unique identifier, without the need to call anywhere or attend in person.

If the testing centre/medical doctor marks the unique identifier as positive, the app anonymously notifies other users who have been in close proximity with the positive user in recent days. The app does not track the user and records only approaches to other users (their location and time), while all users remain completely anonymous.

The app was handed over to all countries free of charge as a tool for health organisations to help flatten the curve and overcome COVID-19 faster. In the future, it will be able to be deployed instantly at the beginning of any other pandemics, to get them under control more quickly. The app will be updated each day, and its developers will cover all expenses. The purpose of the code and know-how is stated to be to help everyone in the world and, therefore, it has been specified that it should not become the property of a single organisation.

Slovenia

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

No COVID-19 specific data protection-related law is in place. The current regulation does not foresee any exception for employers having to comply with the data protection regulation for COVID-19 related reasons.

The Slovenian Data Protection Officer (*Informacijski pooblaščenec*; "**DPO**") has issued several opinions on COVID-19. All of these opinions, views and recommendations regarding the protection of personal data during the coronavirus epidemic (COVID-19) are available here.

Regarding the identification of infected employees, in particular via measuring body temperature, the DPO stated in opinion No. 7121-1/2020/383:

- such measures are possible, however prior consultation with a representative of a medical branch (specifically the designated medical practitioner determining the occupational medicine measures) must be held;
- such measures have to be analysed as to whether they are appropriate and necessary regarding, e.g. the need to protect other employees, and the scope of the collected data has to be assessed and whether storage is appropriate;
- such measures must be analysed on a case by case basis, as general compliance with the data protection laws cannot be taken for granted.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The DPO's general position is that despite the risks associated with the COVID-19 virus, it is not an argument which would lead to the softening of the data protection rules and principles. This is evident as the DPO immediately raised its concern regarding certain public measures that targeted the identification of certain at-risk groups (pensioners, etc.) as they lacked legal clarity on the scope and basis of processing personal data. Furthermore, the DPO also addressed an open letter to the government regarding the use of tracking software without conducting the relevant impact assessments and an analysis of its usefulness. This was also reflected in its opinion regarding the development and use of a mandatory tracking application (opinion No. 07120-1/2020/278). The DPO acknowledged the need for intervention measures in situations as drastic as the current one. However, the appropriate checks-and-balances that protect the rights of an individual from governmental intervention must be kept.

So far no COVID-19 related breaches have been made public.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

Yes, but only between the national health institute and the police. The police can access personal data to determine if individuals are breaching mandatory quarantine orders. This is based on the Intervention Measures to Mitigate the Effects of the COVID-19 Infectious Disease Epidemic on Citizens, the Economy Act and the Government Decision on determining the protocol of personal data exchange between Police, Ministry of health and National institute of public health.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

The Slovenian National Cyber Security Incident Response Centre (SI-CERT - *nacionalni odzivni center za kibernetsko varnost*) has published guidelines on secure remote work.

The key takeaways for employers:

- make employees aware with five pieces of advice for secure work at home (published on the site);
- secure access to the organisation's network;
- update exposed systems;
- analyse if it possible to make a backup;
- create or adapt an incident response plan;
- set up tools for teamwork and make employees aware of them.

The DPO has published guidelines on the protection of data while working from home.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

There are no specific retention guidelines. Therefore, the principle of storage limitation applies. Personal data which is processed for COVID-19 related reasons can only be collected, processed and stored as long as it is necessary for the purposes for which the personal data are processed. It is likely that once the status of epidemic is lifted in Slovenia, companies would need to prove that further collection/processing in this regard is needed.

6. Have any local digital technologies been developed or released in response to COVID-19?

To the best of our knowledge, no public data on local development processes has been made available. We would refer to initiatives at an EU level, e.g. within the eHealth Network (Common EU Toolbox for Member States). Despite its goal in combating the spread of the COVID-19 virus, the outline for the common toolbox stipulated that the essential requirements for national apps will be: (i) voluntary use; (ii) approval by national health authority; (iii) privacy-preservation and (iv) dismantlement as soon as no longer needed.

Turkey

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

There is no specific COVID-19 data protection related law in Turkey. However, some announcements have been made on the Data Protection Authority's ("**DPA**") (*Kişisel Verileri Koruma Kurulu*) website mentioning that personal data will need to be processed during the fight against COVID-19 to prevent the virus from spreading.

Accordingly, it is underlined that the data processing must be made in line with the Data Protection Law ("**DPL**") and must be necessary, relevant to the purpose, restricted and restrained. Data controllers must fulfil their obligation to inform and be transparent about the purpose of data collection and the duration of data storage. All necessary technical and administrative measures must be taken by data controllers and data processors during data processing to prevent the spread of COVID-19, and such data must not be disclosed to third parties if there is no obligation to do so. Data processing for this purpose must be limited and kept at a minimum.

The same public announcement also included a Q&A section where it was indicated that the employer must inform the employees if there is a COVID-19 case in the office. However, the employer must refrain from announcing the name of the infected employee or disclosing too much information considering that the employer is also obliged to act diligently. On the other hand, if there is a specific reason, the employer also has the right to ask its employee whether he/she has visited a region affected by the virus and whether he/she shows any symptoms of the virus. Finally, it was underlined that personal data relating to individuals having the virus can be shared with the relevant authorities.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The DPA announced that there is no legal impediment to public institutions and organisations processing the location and traffic data of individuals in line with the "Pandemic Isolation Follow-Up Project" conducted by the Ministry of Health to prevent the virus from spreading. This project aims to track COVID-19 positive individuals to see whether they act in line with isolation rules required for public health and for the health of their relatives. Accordingly, if a COVID-19 positive individual leaves the house instead of self-isolating, he/she will receive messages on their phones. The information pertaining to those who do not follow the rules will be shared with the police department. Data collected in line with this project will not be used for any other purpose and will be destroyed when the pandemic is over. The government will ensure that such data will not be used for any other purpose and will inspect the security of the system regularly.

Considering that processing location data regarding health status may create risks if obtained by third parties, the institutions and organisations involved in such data processing are obliged to take the necessary technical and administrative measures and delete such personal data on the disappearance of the reason for the data processing.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

There is no mandatory provision specific to sharing COVID-19 data.

However, although the main principle under Turkish Law is to obtain explicit consent from the data subject for data processing, Article 6 of the DPL states that sensitive data relating to health and sexual activity may be processed without obtaining explicit consent from the data subject by persons subject to a confidentiality obligation or by competent public institutions and organisations, for protecting public health, effecting preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Furthermore, pursuant to Article 28(1)(ç) of the DPL, the provisions of the DPL will not apply if personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organisations duly authorised and assigned by law to maintain national defence, national security, public security, public order or economic security. COVID-19 related data sharing with these institutions would fall under this legal basis.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

There are no specific cybersecurity recommendations. However, in an announcement by the DPA, it indicated that all kinds of precautions must be taken, including updating anti-virus systems and security firewalls to condu ct data traffic through secured communication protocols and that employees must be informed in this respect. It is underlined that precautions taken by the employees do not remove data controllers' obligations in terms of security.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

No local law or guidance has been issued in this respect.

6. Have any local digital technologies been developed or released in response to COVID-19?

During the pandemic, it has been seen in certain countries that health, location and contact detail data have been processed for determining individuals who had contact with those carrying the virus or who are at risk of carrying the virus, controlling quarantined individuals, executing curfews and determining busy spots.

The Turkish Ministry of Health has also launched an app for mobile devices with the cooperation of mobile operators and the Information and Communication Technologies Authority, which shows the dangerous zones in cities affected by COVID-19 and the density of infected individuals in each area. It is mandatory for infected individuals and those in isolation to download this app but not for everyone. This app helps to trace users by using their location data, especially those who are affected by the virus, to be able to determine the chain of contact and remind them to stay isolated. Therefore, use of the app is encouraged.

Ukraine

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

No specific COVID-19 data protection-related regulations have been adopted so far. Therefore, the general rules of data protection-related and other laws apply. As a general rule, the consent of data subjects is required to process their personal data. Therefore, when collecting specific information like the temperature of the employees or vendors, such data would likely be considered personal data under the laws and may generally be processed by companies, but only subject to the consent of the data subjects.

In addition, such specific information would in most cases fall in the category of "special risk data". Processing such data generally triggers the requirement to notify the Ukrainian data protection authority (the Ukraine Parliamentary Commissioner for Human Rights, *Уповноважений Верховної Ради України з прав людини*, the "**Commissioner**"). However, on 12 May 2020 the Commissioner released guidance clarifying that employers that process the health data of their employees during the quarantine period are not obliged to notify the Commissioner of such processing.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

Apart from the brief clarification on employers processing their employees' health data mentioned above, the Commissioner has not issued any other guidance or comments to businesses or the public on how to comply with the data protection requirements and data subject rights during the COVID-19 pandemic. The only notable case was on 2 April 2020, when the Commissioner released a statement on its website (link) regarding the mass spamming of citizens via online social messaging services with exact addresses, including apartment numbers, of persons apparently infected with the virus. The Commissioner stressed that any personal data must be processed in compliance with the law and that any breach of this rule may be grounds for criminal or administrative liability.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

No, there are no such specific requirements for private companies.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

On 24 March 2020, the Ukrainian State Security Agency provided, on its Facebook page, cyber security recommendations during remote working. The recommendations include general cyber hygiene points like paying attention to suspicious emails and links, using official software, and having a complicated password, etc. On 7 April 2020, the State Service of Special Communication and Information Protection of Ukraine released a list of more specific technical recommendations to businesses.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

There is no specific regulation or guidance for this. Under the general rule, the methods and duration of processing personal data must correspond to the purpose of the processing. Therefore, the measures requiring COVID-19 related data processing could generally be maintained for the duration of governmental COVID-19 related restrictive measures.

6. Have any local digital technologies been developed or released in response to COVID-19?

On 6 April 2020, the Ukrainian Ministry of Digital Transformation of Ukraine launched an app for monitoring compliance with the self-isolation regime (the "**App**"). All Ukrainian citizens who returned to the country from abroad received a text message with an invitation to install the App. When the App is installed, the person starts receiving push notifications during the 14 days of self-isolation with a request to take pictures. The App then analyses the GPS-location data and, in the event of any non-compliance, sends a notification to the police.

United Kingdom

Please note, both Wales and Scotland have introduced separate legislation to deal with the COVID-19 pandemic.

1. Is there any specific COVID-19 data protection-related law or guidance in your country? In particular, is there a national law (e.g. work safety) which might strengthen a company's position to process personal data for COVID-19 prevention?

The UK has no specific COVID-19 data protection-related law.

All UK employers have a legal obligation to protect their workers and others from risks to their health and safety in the workplace under health and safety legislation. This includes taking reasonable steps to protect workers and others from COVID-19.

2. What is the attitude of the national data protection authorities or other competent authorities regarding this? Are there any notable cases?

The Information Commissioner ("ICO") has published Coronavirus recovery – data protection advice for organisations and specific guidance on Contact tracing – protecting customer and visitor details. The ICO has also published a document setting out its regulatory approach during the COVID-19 pandemic.

Key takeaways:

— The ICO will continue to apply a flexible and pragmatic approach to its regulatory response during the COVID-19 pandemic and recovery phase. However, the ICO still expects organisations to report personal data breaches without undue delay where required by law (i.e. within statutory timeframes), and will take a strong regulatory approach against any organisation breaching data protection laws to take advantage of the current crisis.

— When testing employees, the ICO suggests public task (for public authorities) and legitimate interests are likely to be the most relevant lawful basis for processing. For special category personal data such as health, the ICO suggests that the relevant condition will be the employment condition in Article 9(2)(b) of the GDPR along with the condition in Schedule 1, paragraph 1 of the Data Protection Act 2018 for employer health and safety obligations. This should be assessed on a case by case basis depending on the circumstances, as the employment condition may not always be the most appropriate condition to rely upon.

— Employers must keep records to comply with the accountability principle. Organisations undertaking testing and processing health information should conduct a data protection impact assessment.

— Organisations should keep staff informed about potential or confirmed COVID-19 cases amongst their colleagues. However, organisations should avoid naming individuals if possible, and should not provide more information than is necessary.

We are not aware of any cases where the ICO has decided on COVID-19 related breaches so far.

3. Is there a mandatory provision on sharing COVID-19 data with government authorities?

ICO guidance on Testing emphasises that data protection should not be viewed as a barrier to sharing data with authorities for public health purposes, or the police where necessary and proportionate. Organisations should take into account the risks to the wider public which may be caused by failing to share information, and should take a proportionate and sensible approach. If a member of staff has a positive virus test result, employers and third-party healthcare providers should ensure that the laboratory processing the tests are meeting their legal requirement to notify Public Health England ("PHE").

Designated businesses and organisations, including hospitality, close contact services and leisure venues, are now legally required to log details of customers, visitors and staff to assist the National Health Service ("NHS") Test and Trace. Government guidance states that employers in other sectors should also keep records of staff working patterns for a period of 21 days.

Where there has been more than one case of an employee contracting COVID-19 in a workplace, government guidance states that the employer should notify the local PHE health protection team and follow their instructions including assisting with tracing. If the local PHE health protection team declares an outbreak, the employer will be asked to record details of symptomatic staff and assist with identifying contacts. Employee records should be kept up to date to assist with this.

If there is reasonable evidence that an employee has contracted COVID-19 as the result of an occupational exposure, there may be additional reporting requirements under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013.

4. Are there any cybersecurity or home office recommendations or working from home security requirements?

The National Cyber Security Centre has published specific guidance for home working during COVID-19. This guidance aims to help organisations to reduce the risk of cyber-attacks on deployed devices including laptops, mobiles and tablets, and includes tips to help staff spot typical signs of phishing scams.

The ICO has also published working from home guidance, which includes security checklists for employers.

5. If companies introduce measures which may require COVID-19 related data processing, for how long could they maintain those?

Government guidance recommends that organisations should hold records for 21 days in order to support NHS Test and Trace – and for designated sectors including hospitality, close contact services and leisure venues, this is now mandatory. This reflects the incubation period for COVID-19 (which can be up to 14 days) and an additional 7 days to allow time for testing and tracing. After 21 days, this information should be securely disposed of or deleted. When deleting or disposing of data, organisations must do so in a way that does not risk unintended access (e.g. shredding paper documents and ensuring permanent deletion of electronic files).

If records are made and kept for other business purposes, and are not created solely for the purposes of NHS Test and Trace, there may be a valid justification to retain these after 21 days. However, all processing of personal data must comply with data protection laws, and personal data should not be kept for longer than is necessary.

6. Have any local digital technologies been developed or released in response to COVID-19?

The NHS COVID-19 app is due to launch in England and Wales at the end of September 2020. Scotland and Northern Ireland have deployed their own contact-tracing apps.

Other privately-run symptom tracker apps are also available, including the COVID Symptom Study app that shares data with researchers at King's College London and the NHS.

Your key contacts in CEE & UK

Bulgaria

Nevena Radlova
T +359 2 923 4866
E nevena.radlova@cmslegal.bg

Anna Tanova
T +359 2 921 9940
E anna.tanova@cmslegal.bg

Croatia

Marija Zrno
T +385 1 4825 600
E marija.zrno@cms-rrh.com

Karmen Sinožić
T +385 1 4825 600
E karmen.sinozic@bmslegal.hr

Czech Republic

Tomas Matejovsky
T +420 296 798 852
E tomas.matejovsky@cms-cmno.com

Jakub Kabat
T +420 296 798 750
E jakub.kabat@cms-cmno.com

Hungary

Dóra Petrányi
T +36 1 483 4820
E dora.petranyi@cms-cmno.com

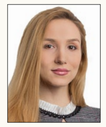
Márton Domokos
T +36 1 483 4824
E marton.domokos@cms-cmno.com

Poland

Tomasz Koryzma
T +48 22 520 84 79
E tomasz.koryzma@cms-cmno.com

Paulina Komorowska
T +48 22 520 8379
E paulina.komorowska@cms-cmno.com

Romania



Alexandra Voinia
T +40 21 407 3815
E alexandra.voinia@cms-cmno.com

Valentina Parvu
T +40 21 407 3825
E valentina.parvu@cms-cmno.com

Russia

Anton Bankovskiy
T +7 495 786 40 63
E anton.bankovskiy@cmslegal.ru

Vladislav Eltovskiy
T +7 495 786 40 90
E vladislav.eltovskiy@cmslegal.ru

Serbia

Jelena Đorđević
T +381 11 3208 900
E jelena.djordjevic@cms-rrh.com

Ksenija Ivetić Marlović
T +381 11 320 8913
E ksenija.ivetic@cms-rrh.com

Slovakia

Martina Šímová
T +421 2221 115 03
E martina.simova@cms-cmno.com

Dominika Mislovičová
T +421 2221 115 21
E dominika.mislovicova@cms-cmno.com

Slovenia

Amela Žrt
T +386 1 6205210
E amela.zrt@cms-rrh.com

Robert Kordić
T +386 1 438 4666
E robert.kordic@cms-rrh.com

Ukraine

Olga Belyakova
T +380 44 391 7727
E olga.belyakova@cms-cmno.com

Mykola Heletiy
T +380 44 391 7732
E mykola.heletiy@cms-cmno.com

Turkey

Alican Babalioglu
T +90 212 401 4260
E alican.babalioglu@ybk-av.com

Inci Alaloglu-Cetin
T +90 212 401 42 60
E inci.alaloglu@ybk-av.com

United Kingdom

Emma Burnett
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

Loretta Pugh
T +44 20 7367 2730
E loretta.pugh@cms-cmno.com