Rödl & Partner

DATA PROTECTION

Covid-19

Data protection Covid-19
August 2020

FREE DOWNLOAD:
www.roedl.it/it-it/it/media/pubblicazioni/documents/dpbites-ebook

FURTHER E-BOOKS:
www.roedl.it/it/media/pubblicazioni/pubblicazioni

PUBLISHER:
Rödl & Partner
Largo Donegani 2
20121 Milano

T +39 02 6328841
www.roedl.it

info@roedl.it

TYPESETTING & LAYOUT:
Rödl & Partner
Corporate Communications
Äußere Sulzbacher Str. 100
90491 Nürnberg

CONTENT

Rita Santaniello
Partner

Nadja Martini
Partner

DEAR READER,

We are living in extraordinary times. In the latest months, everything has been changing and the Covid-19 emergency has been having a deep impact on global economy and business. All companies of any sectors are dealing with this new situation and the legal implications are wide-ranging and complex even from a data protection perspective. Governments around the world are implementing numerous emergency measures focusing, among the others, also on the protection of personal and health data.

In this framework, the issue of urgent measures regarding data protection range from thermo scanner to certifications, from serological test to app tracing.

This E-Book aims at covering all the salient aspects that have characterised this particular period, considering the data protection situation in several countries.

Thanks to the cooperation of professionals from 13 Countries worldwide, we want to provide you with an overview on the main measures and changes that have been introduced during the pandemic. The articles cover the following legislations: Czech Republic, Denmark, Finland, France, Germany, Kenya, Italy, Latvia, Lithuania, Romania, Russia, Spain and Turkey. 13 countries that have come together to address the same issue from different points of view.

Each article taken individually allows you to have a general overview of the situation in the country you are dealing with. At the same time, by reading all the writings, you can understand the general trend, commonalities, new perspectives and get an overall idea of how the protection of personal data is increasingly important within the regulatory framework of each country. Moreover, every article has been divided into different sections, such as: processing of health data and geolocation, pan-European Covid-19 mobile application approach, country specif ic guides to regulate teleworking and data protection obligations.

We hope, with this booklet, to bring you closer to the reality of Data Protection and to give you important notions that are characterising this extraordinary period.

Yours

Rita Santaniello
Partner

Nadja Martini
Partner

1. CZECH REPUBLIC

Prague


Prague
Brno

Processing of health data and geolocation

Based on the COVID-19 pandemic caused by coronavirus spreading also in the Czech Republic, the Czech Government declared a state of emergency that ran from 12 March 2020 to 17 May 2020. During the state of emergency, the Government adopted a wide range of measures limiting various civil rights and freedoms but no measure directly limited the current state of personal data protection based mostly on GDPR. Nevertheless, the pandemic situation has brought new challenges and issues. At the beginning of the state of emergency, the Ministry of Health adopted a measure ordering mobile telephony operators and banks to process operational - localisation data and information about the use of electronic means of payment and to hand over these data to the Ministry of Health or municipal health stations. The purpose of this was to trace and identify the contacts of an infected subject, but free and informed consent of the data subject was required for this. The Government also used mobile phone numbers to send SMS messages about the most important information regarding the state of emergency announced by the Government and the measures introduced.

Currently, the Government and the Ministry of Health inform the public regularly about the number of individuals that are infected, hospitalised, cured and deceased, but only anonymously. The various statistics are based on the anonymous data provided by regional health stations (i.e. authorities responsible for safeguarding public health). Unfortunately, the complicated communication among the state authorities plus certain technical errors have resulted in various discrepancies in published data and have reduced their reliability.

During the state of emergency the Government, in cooperation with private-sector entities, prepared a “smart quarantine” project 1.0. Now the project has been improved and its upgrade version “smart quarantine 2.0” is entirely under control of the Ministry of Health and the National Agency for Communication and Information Technologies. Once the infected person grants their consent, the municipal health station creates a memory map of their locations based on the geo-location data provided by mobile operators. This should help municipal health stations to trace other potentially infected people.

Electronic application – “eRouska 2.0” is one of the important tools that works on a Bluetooth basis and traces the proximity of other users of this application, i.e. those that were in close contact with the infected person. This tracing works only among individuals having mobile phones on which the same application is installed.

Regarding the safety and personal data protection in "smart quarantine 2.0", there is vigorous public discussion on this matter. The Office for Personal Data Protection repeatedly points out that the authorities do not cooperate with the Office properly. Taking into account the fact that "smart quarantine 2.0" deals with the personal data that are processed not only anonymously, the Office strongly recommends preparation of a legal framework for processing such personal data. In addition, the Office points to the insufficiently prepared Data Protection Impact Assessment that has not yet been finalised for either of the planned versions of "smart quarantine". This transaction has already revealed certain risks for the rights and freedoms of the citizens, namely the opportunity to misuse the personal data that must be collected in order to create the currently existing tracing applications.

The Czech Republic would not participate in a European approach regarding development and launching a common app., the Czech Republic is not involved in the Pan-European Privacy-Preserving Proximity Tracing project.

Employer from its employees

Act No. 262/2006 Coll., The Labor Code, requires employers to create a safe and non-hazardous work environment, while taking measures to prevent, eliminate or minimise risks (the so-called preventive obligation). In specific situations, the employer is obliged to proceed in such a way as to prevent, eliminate or minimise risks (he has a so-called preventive obligation).

In times of danger, the employer is therefore obliged to take the necessary protective measures and proceed in accordance with applicable regulations, extraordinary measures of the Government of the Czech Republic and instructions of public health protection authorities. The Ministry of Health of the Czech Republic prepared a manual of possible measures to prevent the spread of COVID-19 in the workplace Information regarding the risks associated with the coronavirus, such as whether they have travelled abroad or encountered an infected person, may be requested from employees. In practice, however, it can be difficult to penalise employees for a false or incomplete answer. An employer cannot enforce coronavirus testing. The Ministry of Labour and Social Affairs of the Czech Republic recommended to the employer to determine the fitness for work of employees through extraordinary occupational medical examinations.

The employer is entitled to keep lists of employees who have become ill with coronavirus and those who are quarantined after their return from a high-risk area. This is the processing of the so-called special category of personal data according to Article 9 of the GDPR, which the employer is entitled to process for the purpose of fulfilling obligations arising from labour law and social security law according to Article 9 (2) (a). b) GDPR. This activity also corresponds to § 101 of the Labour Code, which imposes an obligation on employers to ensure the safety and protection of their employees. Therefore, it is possible to keep records of employees with symptoms of coronavirus or employees who are quarantined after returning from high-risk areas. However, the employer may not publish lists of these employees, he may only publish the total number of quarantined employees.

If an employee has been diagnosed with COVID-19, the employer must, as part of the preventive obligation, inform the other employees about the possible risks in an appropriate manner. However, the facts about a specific person shall be communicated by the employer only to the extent necessary for the protection of health, and so as not to affect the dignity and integrity of that person. Specific data should only be provided to colleagues directly concerned.

Companies from their clients/visitors/providers

The obligation of employees and site visits to undergo temperature measurement is not yet stipulated in any Czech regulation. The person performing the measurement should be instructed in the correct performance of the measurement. It is not recommended to record measured temperatures at this time. Potential outputs should only record decisions whether to allow work / entry into the workplace or not.

Teleworking

An employer has a legitimate reason to monitor an employee who is at the home office, for which he can use, for example, a telephone or software that monitors the time the employee spends using the computer. In order to comply with the principle of transparency, the employer must inform the employee about the inspection. Without sufficient information provided to employees, information about non-performance of work tasks cannot be used for the purpose of corrective measures against the employee (e.g. reproach).

Employers often use cloud storage and access to such storage is often provided by companies outside of the EU. The company that uses such a solution is then responsible for ensuring the legality of the cross-border transfer of personal data. It is strongly recommended that you connect to a video conference only after connecting via a VPN (Virtual Private Network). When sharing files it‘s important to avoid using free storage without adequate security.
If teleconferences are recorded, then only in the sense of the principle of transparency according to Article 5 of the GDPR. It is necessary for the participants in the teleconference to be informed of this fact in advance. Related to this is the need to define the relevant rules (retention period of recordings, purpose, person with access to recordings, etc.).

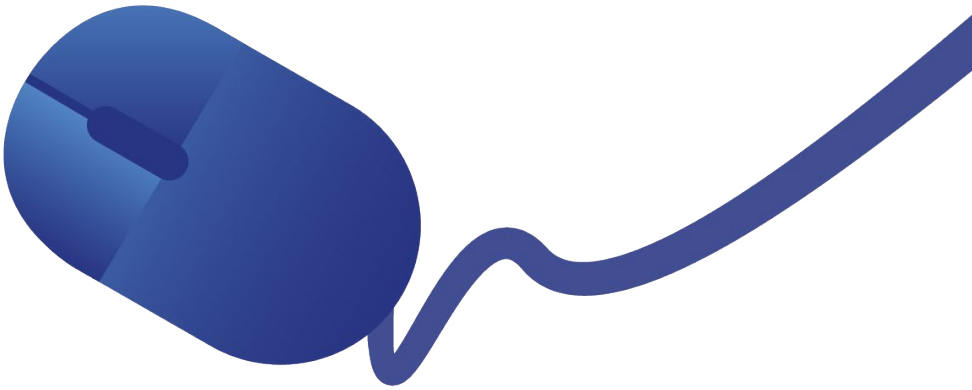
The Office for Personal Data Protection of the Czech Republic has also called on companies to be extra careful when it comes to phishing (typically fraudulent e-mails).

Any other data protection obligations

Generally there are no special rules or exceptions as regards data protection obligations due to the emergency situation. The controllers and processors need to comply as always. Nevertheless the Office for Personal Data Protection encourages the use of contact via telephone and other electronic means for contacting them incl. for reporting data breaches.

Websites protection

As regards website protection, there are no special rules for data protection in connection with the coronavirus situation in the Czech Republic. Companies must observe the statutory rules as always.



Country specifics

Czech Republic: No further specific except for above-mentioned.

Link to the article »

Monika Gardlíková
Attorney at Law (CZ)

monika.gardlikova@roedl.com
T +420 236 16 3111

Lenka Hanková
Attorney at Law (CZ)

lenka.hankova@roedl.com
T +420 775 42 2428

2. DENMARK

Copenhagen


Copenhagen

Data Protection

The spread of Covid-19 has given rise to multiple data protection regulatory issues in Denmark with special regards to the public use of citizens' health information, increased risk of data breaches due to working from home and the Covid-19 app "Smittestop" that will collect personal data in order to prevent further infection.

Health information and exceptions due to Covid-19

In Denmark health information generally enjoys strong protection both from a public and private perspective. The spread of Covid-19 has caused this protection to be temporarily weakened. Not long after the first citizens of Denmark were infected by Covid-19, the Danish parliament introduced a new law that forced physical and legal persons to provide otherwise protected and private data to public health authorities and the police upon request. The order is no longer in force but has been replaced as of 17 April 2020 by a less far reaching order that permits public and private employers to share their employees' identity number in order for Serum Institute of Denmark to offer them a Covid-19 test.

Danish citizens are also protected by the rules laid down in the General Data Protection Regulation ("GDPR"). Furthermore, it is assessed by The Danish Data Protection Agency that private employers can within the boundaries of GDPR register information about their employees in relation to Covid-19 as long as this information cannot be classified as health information as defined by GDPR. The following information can be collected and passed on to public authorities; (i) an employee has returned from an area of risk, (ii) an employee is in quarantined and (iii) an employee is sick.

Smittestop – a Danish Covid-19 app

The Danish public health authorities in cooperation with Netcompany are developing an app in order to prevent further spread expected to be released in May 2020. The app will trace the connection to other users by Bluetooth and thus be able to trace chains of infection and evaluate the risk of infection for the individual. In more concrete terms the app will count how many other users you have been near – that is within two meters distance in more than 15 minutes. The Serum Institute of Denmark will also be able to access the data in order to further evaluate in detail if the social distancing is being complied with. Of course, it is optional if the citizen wants to use the app.

In connection with the development of the app, the Danish Data Protection Agency has expressed the concern that the upcoming app is potentially intrusive in the citizens' privacy, as an app to be used for detection of infections can provide a detailed overview of the citizens' behavior and possibly their health. Therefore, once the app is launched, the Danish Data Protection Agency will focus on verifying that technical solutions in the app have the necessary security and that all data attributable to a given citizen will also be deleted as soon as the extraordinary purpose ceases.

Risk evaluation

Center for Cyber Security in Denmark assess the level of risk of hacking as very high, due to many employees working from home. Many employees working from home give hackers very favorable conditions for tricks such as phishing and many may use services unfit for storing data safely. Public authorities' and businesses' systems are under pressure because of altered use, whilst the availability of them remain even more vital. This combination can lead to a weakening of normal safety procedures.

Therefore, if the employee works from home, it is recommended by the Danish Data Protection Agency that companies, be sure to establish and announce some clear guidelines for working from home. Furthermore, employees should use the designated secure access to professional systems (VPN, direct connection or other secure services). Whenever possible, employees should use the company's management system in place, including access control, document versioning, backup and general security in regard to handling company files.

Link to the article »

Camilla Bjerning Schack
Advokatfuldmægtig
Assistant Attorney

camilla.schack@roedl.com
T +45 2012 3738

3. FINLAND

Helsinki


Helsinki

Authorities in relation to citizens

The European Data Protection Board has 04/2020 provided guidelines concerning the use of location data and contact tracing tool in connection with the Covid-19 pandemic. The guidelines provide the principles that must be taken into account when using location data for preventing the virus. The Board emphasises that the use of contact tracing applications should be voluntary and the main purpose should be keeping distance rather than find out the location.

The Board underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus.

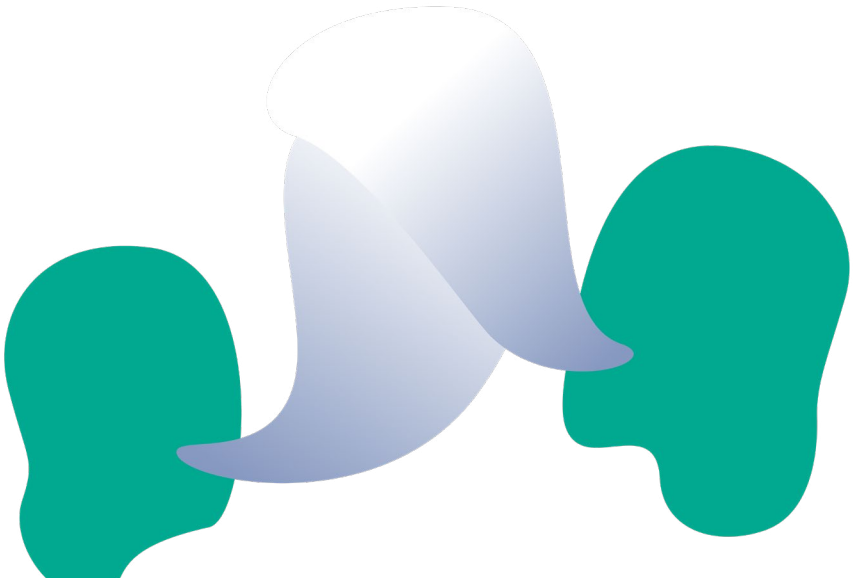
Employer

It is generally permitted to process personal data for the purpose of treating and preventing serious infectious diseases. The employer can collect data concerning the employees' state of health from the employees. The collection of such data from other sources requires the employee´ s written consent. The employee's health data may only be processed by people whose job description includes processing. They are also subject to a confidentiality obligation. If an employee is diagnosed with Covid-19, the employer may not make it public but only inform other employees in general terms and instruct them to work from home.

According to the Finnish Act on the Protection of Privacy in Working Life, examinations and tests concerning the employees state of health shall be performed and taken by health care professionals.

Clients and visitors

The main principle is that like in the rules concerning the employees, examinations and tests concerning the clients and visitors shall be performed and taken by health care professionals. Consent must be obtained.



Data protection obligations

It is important to recognise whether data can be processed by virtue of the GDPR or whether processing will require separate legislation or agreements in addition to GDPR.

For example, in the following cases processing is not possible by virtue of the GDPR alone:

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, for medical diagnosis. Such prosessing requires that the data is only processed by a health professional or person subject to a statutory obligation of secrecy.
- Processing is necessary for reasons of public interest in the area of public health.

Pan-European Covid-19 mobile application approach

Anonymised data on citizens' movements is already available to the government. The government uses this data to support its decision making. The data is obtained by processing communication transmission data which cannot be linked to any one individual. The Chancellor of Justice has concluded that fully anonymised location data does not infringe data protection legislation or any one person's rights.

Any mobile application, however, must be based on consent as it would require the processing of sensitive data. An application must abide by basic rights, such as the right to privacy and the freedom of movement. The data security of any pan-European mobile application would be paramount to ensure no data is leaked. In addition, the data must not be used for any other purpose than to contain the Covid-19 crisis. This is not only to ensure data is processed in accordance with the GDPR but additionally to ensure user confidence in the application.

Teleworking

Country specific guides to regulate teleworking:

- The government has not set any general teleworking guidelines. Each company sets their own guidelines. In general Finland was very progressive with regards to teleworking prior to the Covid-19 crisis. Teleworking had been increasing year by year. Data security and data protection are as important when working from home as working from the office. The employee must ensure that no data, personal or otherwise, is leaked to third parties. In this respect data must not be made available to family members, for example, by leaving papers and notes on tables or not logging out of company computers when not sitting by them.
- Any guidelines set by companies must be abided by. The employee is responsible for securing any data whilst working out of the office.

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

No exceptions to the obligation to comply with the GDPR exist in Finland. Data protection legislation must be complied with in the same manner as prior to the Covid-19 crisis.

Websites protection

Attention to those companies who have seen the urgent need to launch into e-commerce:

- Any company wishing to enter into e-commerce must abide by data protection. In general, where products are shipped directly to consumers, companies shall process personal data (names, addresses, credit card and other payment details).

Country specifics

The Finnish Act on the Protection of Privacy in Working Life govern employee and employer relations with respect to data protection including the collection of health-related data.

Link to the article »

Pekka Pulli
CATL

pekka.pulli@roedl.com
T +358 0 5033 69 343

4. FRANCE

Paris


Paris
Strasbourg

Processing health data Collection of employee health data within the framework of Covid-19

The French data protection authority (the CNIL) has edited recommendations for employers about what they can do and what they cannot do in accordance with the GDPR and the French data protection act and in order to respect the employees' privacy.

Information about employees' health are classified as "sensitive personal data", in the sense of article 9 of the GDPR, and the processing of these data is particularly supervised.

Employers can process health data relating to a data subject where it is necessary for the employer to comply with its legal obligations in relation to health and safety. Even in case of an epidemic, key principles of the GDPR must apply.

If contamination is reported, employers can collect some data such as:

- The date and the identity of the person suspected of having been exposed;
- The organisational measures taken (containment, teleworking, orientation and contact with the occupational physician, etc.);

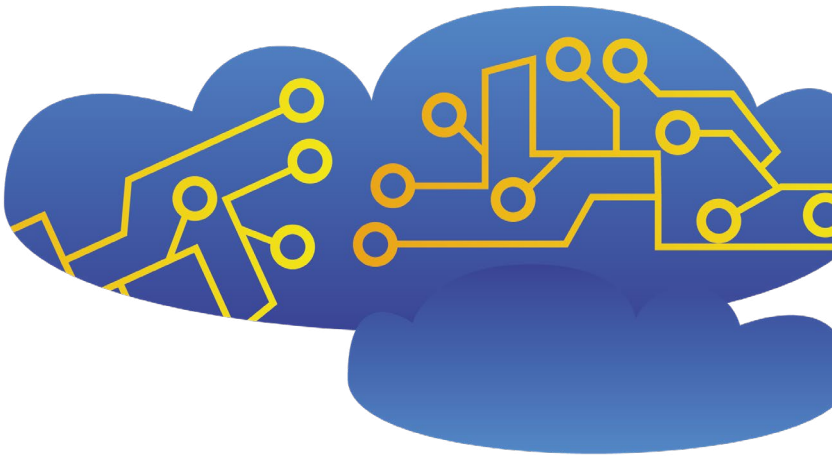
Employer will thus be able to communicate to the health authorities, at their request, the information relating to the nature of the exposure necessary for any health or medical care of the exposed person and also to limit contamination.

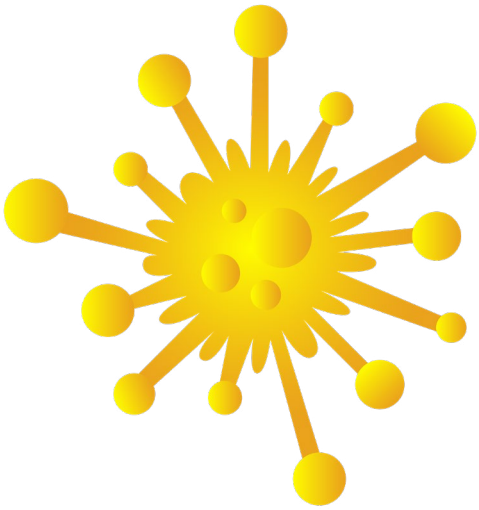
According to the CNIL, it is not possible to collect data in a systematic and generalised manner, or through individual inquiries and requests, to seek possible symptoms presented by an employee or his / her relatives.

For example, it is not possible to:

- Take daily temperature readings of its employees or visitors;
- Ask its employees for their medical records;
- Collect and process information about the health of the relatives of employees.

These recommendations are likely to change as the spread of the virus progresses. In this regard, it is recommended to keep informed through the Government's website and to be attentive to officials guidelines.





Teleworking

The health crisis linked to Covid-19 has led several companies to set up, sometimes in a hurry and in a disorganised manner, telecommuting in order to preserve at least part of their activity. An uncontrolled implementation of telework accentuates the risks in terms of security for the companies that resort to it (information theft, fraud, ransomware, etc.).

This can go as far as putting the company in pure and simple danger in regards to cybercriminals who try to take advantage of a vulnerability and the dematerialisation of nearly all of the company's internal procedures.

WHAT ARE THE RISKS?

Phishing
These are messages (emails, SMS, etc.) that aim at stealing confidential information (passwords, bank details, etc.) by impersonating a trusted third party (colleague, superior, etc.). This practice can lead to the hacking of e-mail accounts, access to information systems, false orders or false transfer orders, etc.

For example, on the 21 March, a French wholesaler working for pharmacies was offered an order of more than six million euros in hydro-alcoholic gel and masks by swindlers posing as a supplier known to the company.

Hostage-taking of information systems or ransomware
This type of attack consists in encrypting or preventing access to the information system of the company in exchange for a ransom payment. This type of attack may be accompanied by data theft or prior destruction of backups, as well as by suspending affected company's activity.

As an example, on 22 March, the Paris Hospitals (AH-HP) were fell victim to a cyber-attack by a massive connection on their servers. Although the attack was brought under control by the AH-HP, this type of attack is likely to become widespread and concern both public institutions and private companies.

Data theft
This type of attack consists of breaking into the company's information system in order to steal data with the aim of blackmailing it by threatening to resell it or distribute it to third parties in order to harm the company. This can lead to a suspension or even a total halt of activity, depending on the data concerned, as well as damage to the company's image and reputation.

WHAT ARE THE BEST PRACTICES AND MEASURES TO ADOPT?

As the activity of most companies is already impacted by the health crisis, preserving the security of the information system, which is at the heart of their operations, must be a priority. You will find below a non-exhaustive list of recommendations and good practices, which will have to be adapted on a case-by-case basis:

Reinforcement of security measures to detect or prevent cyber-attacks
Each company should work with its CIO and / or CISO and / or IT service provider to strengthen authentication procedures (stronger passwords, double authentication if possible) and check that all security updates are carried out, etc.

Use of professional tools
It is advisable for each company to provide as far as possible professional tools to teleworking staff and avoid the use of personal equipment (mobile phones and computers) whose security level is often faulty or difficult to control.

Awareness raising of teleworkers
The following recommendations, among others, should be communicated to staff:

- Exercise caution in regards to messages of unknown or unexpected origin (e.g. mentioning a good deal, a refund, an order confirmation, etc.);
- Be aware of the risk of false orders or changes in bank details (always check the information with the person in question by other means);
- Make updates (especially security updates) as soon as they are available on all connected equipment (servers, telephones, computers, etc.);
- Download only applications authorised by the company (on professional hardware) and through official platforms;
- Make regular backups of data and keep a disconnected copy;
- Notify the hierarchical superior or the IT department in case of doubt;
- Remind them, if necessary, that the IT charter may provide for sanctions in the event of non-compliance with its provisions.

WHAT TO DO IN THE EVENT OF FRAUD OR A CYBER-ATTACK?

In case of fraud or a financial scam, the company must act quickly and contact its bank in order to block the last transfer made, within 24 to 48 hours.

Any fraud or financial scam making use of the internet must be reported on the PHAROS platform set up by the Government. Finally, in case of data violation (breach, hacking, etc.), companies must notify the CNIL within 72 hours

Relations with the CNIL during a state of health emergency

The CNIL has announced, through a communication of 17 April, that its activities were not suspended despite the situation and that it intended to minimise the slowdown.

The CNIL has indicated that it will give priority to dealing with cases related to the Covid-19 epidemic. It has indicated that it will nevertheless carry out all of its missions and minimise the slowdown in its activities. Lastly, it indicated that most of the time limits granted to its users to respond to its requests or decisions are extended to take account of this exceptional context.

Link to the article »

Leila Benaissa
Senior Associate
Advokat / Attorney at Law

leila.benaissa@roedl-avocats.fr
T +33 1 5692 3914

5. GERMANY

Nuremberg


Hamburg
Berlin
Bielefeld
Muenster
Dresden
Chemnitz
Cologne
Jena
Hof
Plauen
Eschborn
Selb
Bamberg
Bayreuth
Fuerth
Nuremberg
Mettlach
Ansbach
Ludwigshafen
Regensburg
Stuttgart
Ulm
Munich

The legal regulations for combating the pandemic in Germany are complex, since in addition to the requirements of the epidemic response at federal, state and local level, there are also regulations on occupational health and safety, both general and sector-specific. In addition, the regulations at all levels are constantly being updated and adapted, which makes it difficult to maintain an overview.

Processing of health data and geolocation

- Currently, there are no general legal obligations in Germany to collect health data (temperature measurements) for access to facilities. With regard to contact tracing, regulations have been issued in some federal states that provide for the collection of data in certain areas (restaurants) and can be regarded as a legal basis within the meaning of the GDPR. In addition, occupational health and safety regulations recommend the documentation of visitors and their contact details to enable contact tracking; in this case the legal basis under data protection law is unclear.
- Individual GPS tracking is not used because it is deemed unsuitable. Anonymised mobile phone localisation data were used by the German epidemic control agency to understand the slowing or acceleration of population movements.
- Mandatory temperature measurements of employees, suppliers or visitors are controversial in terms of data protection. Since the highest risk of infection already exists two days before symptoms appear, and since the illness, with the risk of further infection, sometimes occurs completely without symptoms, temperature measurements appear to be of only limited use and may therefore not be necessary. At best, they can be considered as supplementary measures and especially if local events (either in the affected company or in the region) show an increased risk of infection. Supervising authorities are currently investigating supermarkets that have used thermal scanners for all visitors.

Pan-European Covid-19 mobile application approach

The German government supports the Pan-European Privacy-Preserving Proximity Tracing Initiative (PEPP-PT), in which, among others, two leading German scientific institutes are involved. The Corona app, based on a decentralised software architecture, is being developed by Deutsche Telekom and SAP. Interoperability with other European solutions is to be worked to achieve. The app is to be optional for German citizens, comply with the applicable data privacy regulations and ensure a high level of IT security. It will also have an anonymous, cross-national exchange mechanism for travel between countries. In terms of functionality, the app will record which smartphones have come close to each other and store the epidemiologically relevant contacts of the past three weeks. Users are to be warned if it turns out that they were next to infected persons. Technically, this will be done via Bluetooth ID exchange between mobile phones. Part of the tracking data will be stored in the smartphone, another part will be distributed to several independent servers, each of which will receive only a small amount of sensitive information. This is to prevent data misuse. However, there are still concerns about data protection law, and there is still no official data protection impact assessment. Supplementing laws regarding liability or to strengthen the free consent for the use of the app are not considered now.

Teleworking

Ccountry specific guides to regulate teleworking:

- There are no specific German regulations regarding data protection when teleworking. Therefore, the general measures apply. Companies have to take into account the changes of operations and adjust their risk assessments, policies, processing register etc. accordingly.

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

- There are no statutory changes regarding data protection obligations.
- Some of the regional German Supervising Authorities at the moment generally accept (https://www.datenschutz-bayern.de/corona/sonderinfo.html) the use of personal devices of employees for video conferencing or messaging between employees as well as towards customers, provided that at least certain privacy requirements are fulfilled (password protected devices, data minimisation, etc.). The commitment, which applies only to certain branches and regions, has already be prolonged, now until 14 June 2020.
- Other Supervising Authorities (https://datenschutz-hamburg.de/pages/corona-faq) stated not to issue fine notices in ongoing fine proceedings for the time being in order to ease the burden on companies and tradespeople in the current process of adapting to the numerous changes resulting from the corona crisis.
- Some health authorities on request gave lists with the contact details of infected persons to police services, which was considered by all the regional Supervisory Authorities to be an unjustified processing of health data under the GDPR.

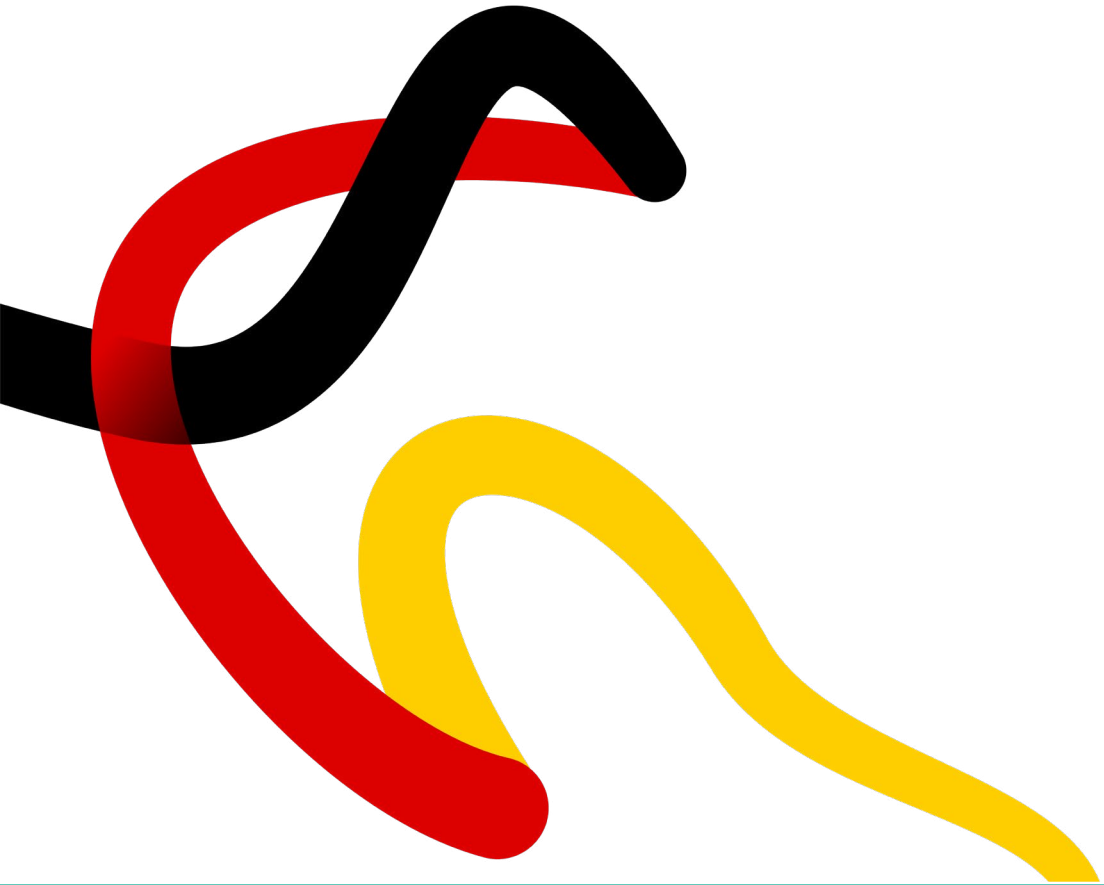
Websites protection

Attention to those companies who have seen the urgent need to launch into e-commerce:

- Identity theft occurred on a larger scale during the 1st phase of state support measures. It was relatively easy for companies to apply for subsidies or loans via websites operated by federal states, which were granted quickly. Since identity verification was initially neglected, fraudsters took advantage of these support services by demanding by demanding (and receiving) payments for existing companies themselves.

Country specifics:

There are currently no specific changes in German privacy law.



Link to the article »

Alexander von Chrzanowski
Associate Partner
Rechtsanwalt

alexander.chrzanowski@roedl.com
T +49 3641 4035 30

6. ITALY

Rome


Bolzano
Padua
Milan
Rome

Processing of health data and geolocation

- Authorities in relation to citizens: technologies (termoscanner, drones, smart cities, thermal camera, swabs, sierological tests, medical certificate, etc.) and applications for contact tracing implemented in the respective countries / privacy by design, telecommunications' metadata (duly anonymised would be out of the scope of the GDPR but still requires security and confidentiality obligations), self-declaration models.
- Employer from its employees: return to the workplace, measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc. Attention on: Privacy statements, PIAs, risk assessments, data register, purpose limitation, integrity and confidentiality, proportionality and data minimisation, privacy statements, organisational and technical measures;
- Companies from their clients and visitors: temperature measurements, etc.
- Companies from their providers: measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc, organisational and technical security measures

Italian DPCM of 26 April 2020 and the Protocol of 24 April 2020 allow the employer to take appropriate measures to control the access of employees, suppliers and visitors to workplace.

The employer may subject the staff to a body temperature check before entering the workplace: when temperature exceeds 37.5°, access to the workplace will not be permitted. Persons in this condition will be momentarily isolated, provided with masks and will not have to go to the Emergency Room and / or to the infirmaries, but they will have to contact their doctor as soon as possible and follow his indications.

The employer shall inform the staff in advance, and those who intend to enter the company, of the foreclosure of access to those who, in the last 14 days, have had contact with people who have tested positive for Covid-19 or come from areas at risk according to the WHO guidelines.

Moreover, the entry into the company of workers who have already tested positive for Covid-19 infection must be preceded by a prior communication with a medical certificate that shows that the swab has been "negativeised" in accordance with the procedures provided for and issued by the territorial prevention department of competence.

Finally, the swabs and serological tests shall only be ordered by the health authority. In particular, in case of serological tests, the employer must cooperate to ensure that employees undergo them.

Pan-European Covid-19 mobile application approach

Following the analysis work of a Task Force, the Extraordinary Commissioner has identified in "Immuni" the App for the fight against virus infection. The processing of personal data has been subject to evaluation by Italian Supervisory Authority and, therefore, stated by Article 6 of Law Decree no 28/2020. In particular:

- The data controller is Ministry of Health which coordinates with other actors (including data processors) between public administrations and health authorities;
- The data subjects receive, before the activation of the application, in accordance with Articles 13 and 14 of GDPR, clear and transparent information in order to achieve full awareness, in particular, of the purposes and processing operations, pseudonymisation techniques used and data retention times;
- By default, the application collects only personal data necessary to warn users of the application to fall within the close contacts of other users found positive to Covid-19;
- the alert system is based on the processing of proximity data of the devices, made anonymous or, where this is not possible, pseudonymised; in any case, the geolocation of individual users is excluded;
- Data relating to close contacts are stored, including in users' mobile devices, for the period strictly necessary for processing, the duration of which is established by the Ministry of Health; the data are deleted automatically upon expiry of the period;
- The data collected through the application may not be processed for further purposes, except for the possibility of use in aggregate or anonymous form, for public health, prophylaxis, statistics or scientific research purposes only;
- The non-use of the application does not entail any prejudicial consequences and the respect of the principle of equal treatment is guaranteed;

The use of the application and the platform, as well as any processing of personal data carried out pursuant to this article, shall be interrupted on the date of termination of the state of emergency, and in any case no later than 31 December 2020, and by the same date all personal data processed must be deleted or made permanently anonymous.

Teleworking

Country specific guides to regulate teleworking:

- Update of risk analysis, privacy impact assessment, data register due to the teleworking situation: Smart working;
- Design of teleworking policies / policies on the use of tools and devices: annex to workers' contracts; flyer and procedure;
- Security measures on company's information systems and Cybersecurity measures (secure teleconferencing, arising awareness) relating to teleworking device: specific guidelines;
- Implementation of employee performance monitoring measures and related activities: assessment of the risks, PIA, duly inform, ROPA update;
- DPCM 26 May 2020 recommends that employers encourage smartworking except where it is necessary to go to the company's premises to perform the work.

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

- Remotely handling and reporting of security breaches: specific communication channels for breaches or severe cases of security breaches in the different countries;
- Attendance of the rights requests should be especially observed. Added difficulties since there are fewer resources and possibly more attention is being given to other issues;
- Contracting with new providers, especially digital / cloud services and products, must involve privacy and security reviews.
- Constant changes and faster operations than usual cannot lead to the disregard of information obligations, PIA's, risk assessments, updating ROPA, etc.

Article 17-bis of Law Decree no 18/2020, converted in law by Law no 27/2020, states some derogations for health authorities involved in combating the virus. In particular:

- The disclosure of special categories of personal data between heath authorities is permitted;
- The information ex Article 13 GDPR may be omitted or provided in a simplified form;
- Instructions to persons in charge of the processing activities may be provided in oral form

At the end of the state of emergency, the health authorities will take appropriate measures to bring the processing of personal data carried out in the context of the emergency back to the ordinary competencies and rules governing the processing of personal data.

Websites protection

Attention to those companies who have seen the urgent need to launch into e-commerce:

- Cyberattacks: web-specific security policies
- Adaptation of the legal texts required on a website, privacy policy, legal notice, cookies, T&C's, etc.

Country specifics

- Italy: Local Laws relating to processing operations of employee's and provider's data: from smartworking up to apps, swabs, sierological tests, medical certificate; Local laws relating to Covid apps.
- Spain: Observance of digital rights in times of Covid-19.

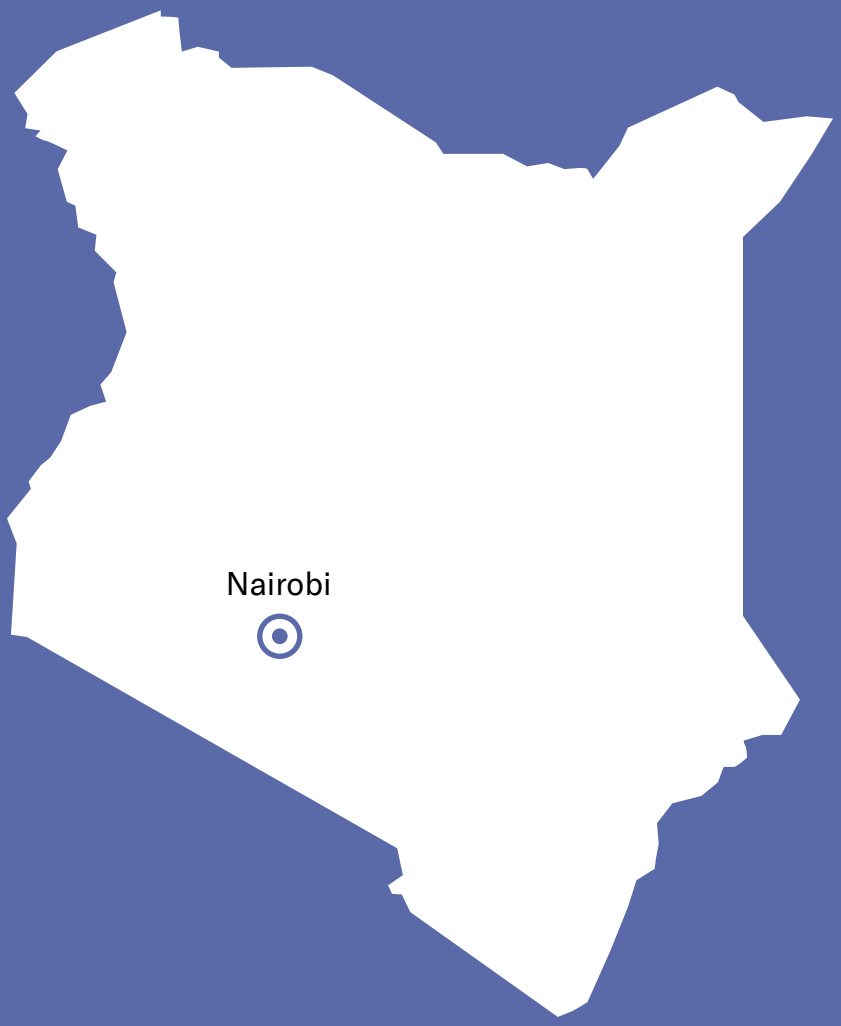
Link to the article »

Nadia Martini
Partner
Avvocato

nadia.martini@roedl.com
T +39 02 6328841

7. KENYA

Nairobi


Nairobi

Kenya's confirmed Covid-19 cases reached 700 people at the start of the second week of May 2020, well within the numbers the region is reporting, though far from the tens of thousands reporting across Europe and the United States. Nevertheless, Kenyan health authorities have consistently maintained the need to ensure confidentiality of patients personal identifiable data is maintained, citing both doctor-patient confidentiality, as well as confidentiality on account of personal data and privacy laws.

Below, we address some key personal data protection concerns and considerations that businesses ought to have when implementing the use of most wide-spread 'health check' on people (visitors, employees etc), that is, the thermo-scanner and similar checks.

Processing of health data

The World Health Organisation lists fever among Covid-19's most common symptoms, which has led to prevalent use of thermo-scanners (temperature guns) prior to entry into many of Kenya's malls, stores, commercial premises, and even parks and forests , all of which have generally remained open as Kenya did not enforce a full 'lock-down'. Many workplaces are taking and checking employees' body temperature at least once a day, with the general assumption being that body temperature above normal is indicative of illness, and in these times, may indicate Covid-19 infection.

Whilst not immediately apparent to many businesses in Kenya, temperature and any other body measurements are a type of 'health data', defined in the Data Protection Act as data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services. As such, Coronavirus symptom-checkers like temperature measurements ought to be regarded and treated as incidents of processing of personal data, and accordingly, should be conducted in-keeping data protection rights and principles. These include the following:

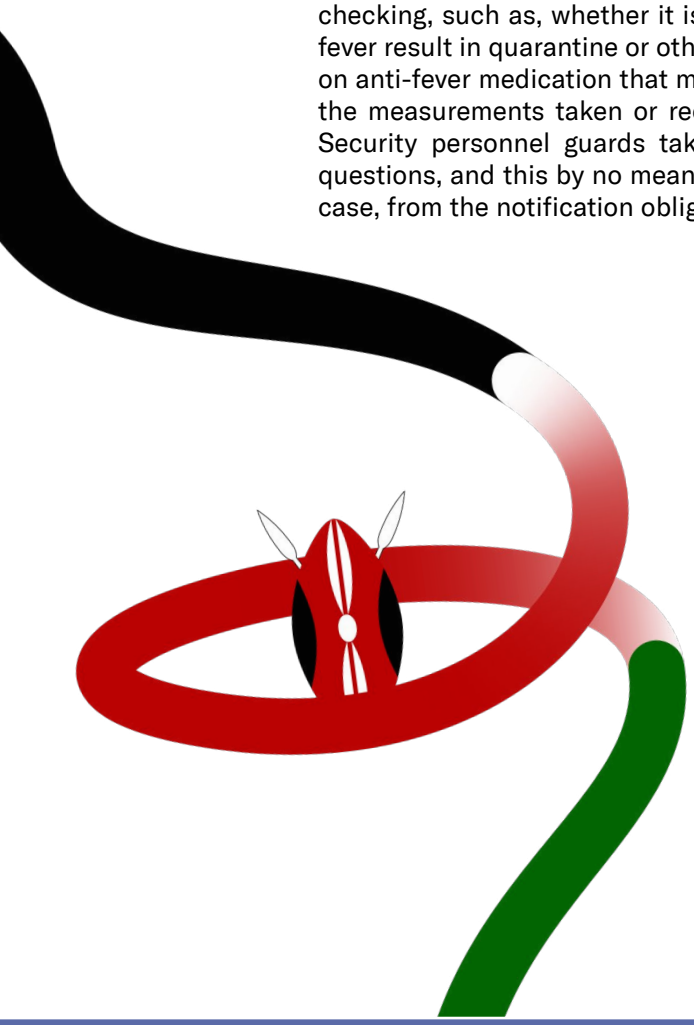
<u>Privacy</u>
Most workplaces and commercial premises are leaving temperature-checking to security personnel and guards at building / office entrances, a process that is almost always absent of any privacy whatsoever, and with companies' Human Resources personnel practically completely removed from the process. We recommend reconsidering this, and for example in offices, involving only HR personnel in such exercises. observing employee privacy when taking the measurements.

Accuracy

Many of the thermos-scanners in use are simple handheld devices. It is important that employers and business owners ensure that the devices are reasonably in good working order and are used correctly, in order to take accurate measurements. Whilst inaccurate temperature measurements may not normally have serious consequences (particularly because thermos-scanners are usually used in health facilities where several diagnostic tests are likely to be conducted upon a finding of fever), in the wake of Covid-19, a higher than normal temperature measurement may result not only in an incorrect assumption of having the virus but additionally result in an employee or visitor being quarantined, with resultant economic and psychological consequences.

Notification

Most business premises are not providing sufficient information regarding temperature checking, such as, whether it is pre-requisite to entry, the result of a particular finding (will fever result in quarantine or other further testing?), asking whether or not the subject may be on anti-fever medication that may reduce the efficacy of the result, informing about whether the measurements taken or recorded are stored and if so for what purpose and duration. Security personnel guards taking measurements are likely ill-equipped to answer these questions, and this by no means exempts the business / employer, the data controller in this case, from the notification obligations in the Data Protection Act.



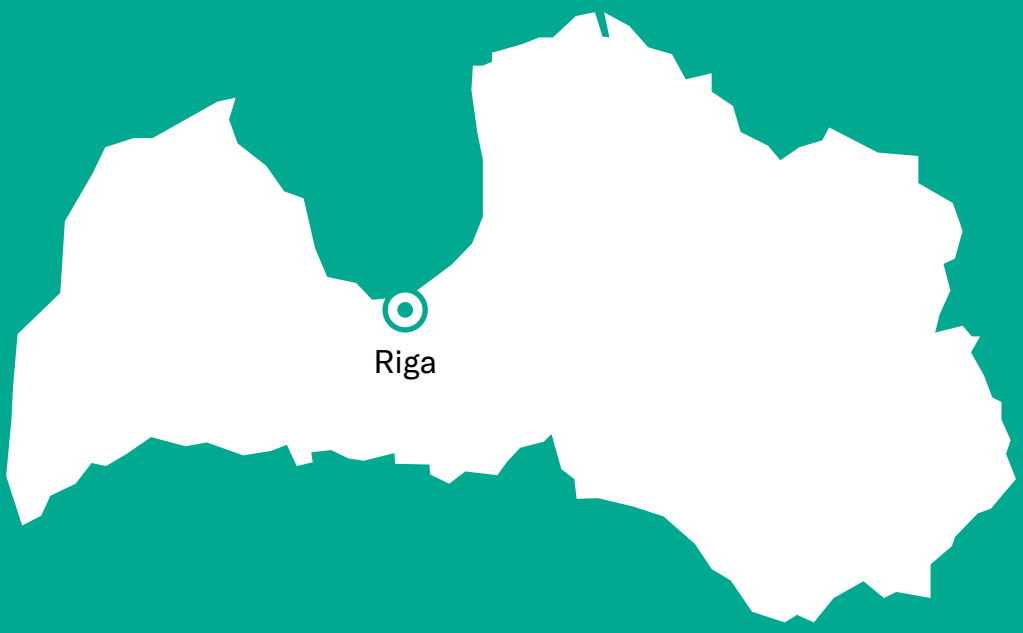
Link to the article »

Penninah Munyaka
Associate Partner

penninah.munyaka@roedl.com
T +254 702 4632 72

8. LATVIA

Riga


Riga

Pursuant to the World Health Organisation Statement dated March 11, 2020 according to which COVID-19 has become a pandemic, and on the basis of several national security laws, the emergency situation had been declared from March 12 until 9 June, 2020 in the territory of the Republic of Latvia, with the purpose of containing the spread of COVID-19.
As a result, the Latvian government implemented enormous amount of changes in the national regulations, inter alia changing regulatory acts and provisions relating to personal data processing matters. Rödl & Partner Riga office would like to provide information regarding data processing provisions, guidelines, and practice in Latvia.

Processing of health data and geolocation

Authorities in relation to citizens:

According to the decree of the Cabinet of Ministers "Regarding Declaration of the Emergency Situation" dated 12 March 2020, the persons who had been determined by the Centre for Disease Prevention and Control as contact persons of the COVID-19 infectious disease had to:

- self-isolate at the place of residence (home quarantine) for 14 days and be available for contact and cooperate with the family doctor and other medical practitioners. During this period they had to stay at the place of residence, were not allowed to go to work, community and public places, as well as to places where a large number of people were present;
- observe their health condition for 14 days and measure body temperature twice a day (in the morning and in the evening);
- call the emergency number without delay if any signs of acute respiratory infection occurred (cough, increased body temperature (fever), shortness of breath);
- avoid putting other persons at risk of infection by reducing direct contact with other persons (avoid welcoming guests, do not visit other people, do not use the public transport, etc.);
- use any of the possibilities to purchase basic necessities or food remotely (by door-to-door delivery, avoiding contact with the supplier; delivery of food or goods which is ensured by relatives by leaving the purchased products at the door; requesting assistance of the local government social service);

As regards to the persons who had arrived from foreign countries, except Lithuania and Estonia, or for whom the COVID-19 diagnosis had been confirmed and whose health condition allowed to undergo medical treatment at home, they had to be under strict isolation, observing aforementioned movement limitations. In the event of a healthy recovery the isolation could have been discontinued only with the permission of the attending physician.

The most important state institutions, which were responsible and entitled to process health data and geolocation of citizens during the emergency situation, were as follows:

- Centre for Disease Prevention and Control,
- Health Inspectorate,
- State Police and the municipal police.

The Health Inspectorate in cooperation with the State Police and the municipal police had the authority to control the execution of the above listed requirements. The Centre for Disease Prevention and Control was entitled to transfer personal data (name, surname, personal identity number, telephone number, the address of the place of quarantine and the actual place of residence) to the Health Inspectorate, the State Police, and the municipal police or ensured that the abovementioned institutions had access to the respective personal data.

In order to monitor and ensure that persons comply with the imposed movement restrictions, telecommunication companies were providing geolocation data of their customer's mobile devices upon written requests from authorised state institutions. In this regard, service providers publicly announced that it was not possible to determine the exact location of each person because only an approximate location, which is matching the territory of a football pitch, can be traced. A representative of other service provider emphasised that the mobile operator did not track the location of its clients, but, upon a justified request, the location of a person could be determined, by analysing the information from the base stations to which the customer's device was connected. The State Police and the municipal police had the right to search for the persons who were obliged to observe self-isolation or quarantine, and, if they were ignoring it, also had the right to forcibly convey the abovementioned persons to the place of quarantine or the actual residence, as well as to impose monetary sanctions.

These data processing activities were performed mainly for a certain group of persons that were recognised as potential carriers of COVID-19. There was no other publicly available information concerning government's personal data processing that was not anonymised in connection to geolocation of persons. Anonymous data were used by state institutions for statistical and intelligence purposes, as well as administration of COVID-19 spread in the territory of Latvia.

In June 2020 a new app called "Apturi Covid" (Stop Covid – in English) was launched. The use of this app was and still is completely voluntary. The technical solution involves activation of Bluetooth Low Energy that under certain circumstances (a distance of less than 2 metres between two users, duration of a contact for at least 15 minutes, both users have downloaded and activated the app on their devices) establishes a contact between two devices. A person infected with COVID-19 infection obtains a unique code from the Centre for Disease Prevention and Control and activates it in the app. When the contact of two devices is established and one of the users has activated this unique code, a person who has been in contact with the infected person receives an automatic notification about the possible infection risk. Information about possible contacts is saved only in the app and is erased automatically after 14 days.

The data controller for the data processed by the app is the Latvian Centre for Disease Prevention and Control who processes the following data: date of the contact, duration of the contact, strength of the signal and a user's phone number (the last one is optional). The users do not receive any data regarding other users. If a user has opted to indicate his contact information (a phone number), the Centre for Disease Prevention and Control will contact the user in case there is notification about the possible infection risk. If the user does not receive any notification, the Centre for Disease Prevention and Control will not receive and process any information about the user.

In addition, the national supervisory institution – the Data State Inspectorate, instructed state institutions that, when publishing information about new places where COVID-19 has spread, the respective information could be published strictly in a way that it does not allow to identify specific patients or contact persons. For instance, if any institution plans to publish a map of COVID-19 spread, the responsible authority may do so by indicating the city or town in question with a larger population.

Temperature measurements:

Due to COVID-19 outbreak and in order to protect personnel, clients and visitors, companies are conducting temperature measurements on a daily basis. It shall be noted that there are no any specific regulations introduced for processing of such health data of the personnel or third parties in Latvia.

As it was explained by the Data State Inspectorate, temperature measurements could be seen as a precautionary measure that meets the requirements of the GDPR, as long as the results of temperature measurements are not stored anywhere or being made available to others. Also, supervisory institution advises to refrain from default temperature measurements and advises, instead, just ask the employees, whether they have symptoms of COVID 19 or they have been diagnosed with COVID-19, and then, if necessary, measure temperature.

Nonetheless, according to the Latvian labor regulatory acts, it is the duty of the employer to ensure working conditions that meet the requirements of occupational health and safety. This also means that it is the employer's responsibility to ensure that his negligence does not cause his employees to fall ill as a result of the virus circulating at work. In the same time, every employee must act responsibly towards his / hers workplace and inform the employer without hesitation if he / she is infected or at risk to fall ill. In the light of such prudent actions employers are also entitled to ask employees, whether they have been abroad during the last 14 days and have / have not been in contact with patients diagnosed with COVID-19 or contact persons thereof.

Practical problem with temperature measurement is that temperature measurements are not always performed in suitable places. For example, in one supermarket chain, temperature is being measured of everyone before entering the store. Due to weather conditions, clothing, peculiarities and characteristics of the person, etc., temperature measurements are quite inaccurate, which may also give a misleading impression of a person's true health condition. Nonetheless, in Latvia, here it is the most commonly used health data processing measure to fight and try to contain the spread of COVID-19.

Other data processing measures:

Referring to relations between companies and their clients, visitors, as well as suppliers, Latvian supervisory institutions have developed general guidelines on what would be considered a good practice. Companies related to high intensity of human flow (retailers, grocery shops, pharmacies, shopping centres, etc.) were required to provide additional security measures at cash desks and monitor flow of visitors to avoid crowding. As regards to the latter, video surveillance is considered a main data processing instrument used for monitoring people. Given that CCTV itself requires data protection impact assessment, for companies where CCTV is already in place, it is relatively easier to integrate a new purpose of personal data processing within existing policies.

It is known that in certain business sectors, for instance, in supply chains, the contracting parties require the other party and its staff to certify that they comply with the imposed restrictions. Employees visiting the office or business premises or couriers delivering products should be declared healthy and parties have to immediately inform each other in case any of its employees are being diagnosed with COVID-19. Nonetheless, companies are required to protect personal data of its employees against any unnecessary exposure. As a good practice could be considered informing the contracting party about the approximate time of the day, arrival, duration of presence of the infected employee, so that the other party have enough information to react and address this issue with its employees who potentially had been in contact.

TELEWORKING

As mentioned before, the emergency situation has been declared in Latvia from 12 March until 9 June 2020. During the emergency situation, the state and local government institutions, as well as state owned companies had to assess and ensure, to the extent possible, the remote provision of on-site services.

In addition, in order to ensure safety of persons working in private sector and mitigate the risks of the COVID-19 outbreak, the government encouraged companies to work from home. Of course, businesses that are not tied to offices did not feel the transition to teleworking as much as those which do their day-to-day operations at offices, e.g., accountants, lawyers, sales managers, financial advisers, etc. Nevertheless, most of professions had the ability to adapt to new challenges, inter alia adjusting internal business processes, policies, designing new or using existing technical tools in order to continue business operations, provide services and maintain activity throughout this time.

The Data State Inspectorate issued the following guidelines:

Devices

Employees shall take special care to prevent devices such as flash drives, memory sticks, cell phones, laptops, or tablets from being misplaced or lost. Also, it is essential to ensure that computers, laptops, or other devices used for work are in a secure place or not left unsupervised and, during the work, any chances of other people seeing the device screen are minimised.

As regards to technical configurations, devices must have the necessary updates, such as operating system, software, antivirus updates. An effective access control system (i.e. multi-factor authentication and secure passwords) shall be used to restrict third-party access to the device, preferably ensuring encryption. Devices should automatically lock if for any reason they are left unattended, and, in case of theft, the device should immediately delete all data and clear the memory or it could be done remotely.

Emails

Companies have to implement internal policies for personnel and employees must comply with the rules on the remote use of work emails. Person's work emails shall be used to perform only work-related duties, therefore, employees must make sure they send or receive any content of private matter on personal email addresses. In addition, no private information should be stored on devices provided by the employer solely for work purposes.

When sending emails, employees have to be sure that the recipient is indicated correctly, especially for emails that contain large amounts of personal data or sensitive personal data.

Cloud computing and network access
Organisations shall use trusted network or cloud services, whereas the personnel is instructed to follow internal rules and procedures for network or cloud access and data sharing within one organisation or when communicating externally. If it is not possible to use trusted network or cloud services, organisations, particularly all employees, shall ensure that all locally stored data is properly backed up in a secure way.

DATA PROTECTION OBLIGATIONS

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always

Despite the emergency situation, the position of the Latvian Data State Inspectorate had not changed. Namely, even during the emergency situation, the requirements of GDPR must be strictly observed, personal data must be processed and information must be provided to data subjects in accordance with the provisions specified in applicable laws.

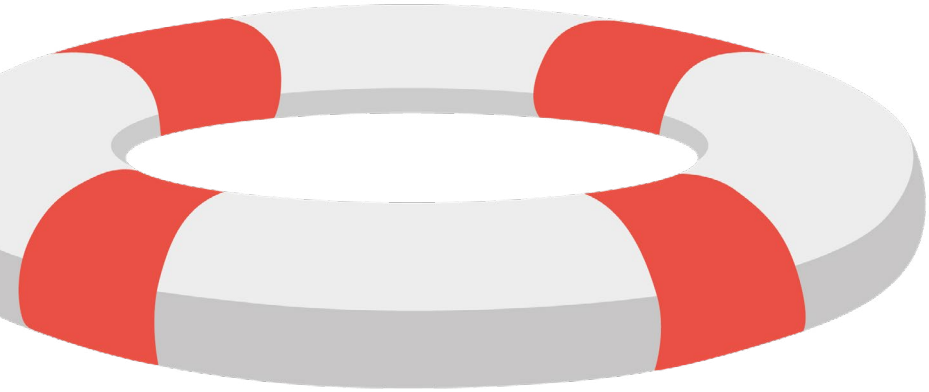
WEBSITES PROTECTION

Attention to those companies who have seen the urgent need to launch into e-commerce

It is no secret that COVID-19 is a huge opportunity for the development of e-commerce, helping companies, especially merchants, to overcome current situation.

Earlier and now, e-commerce in Latvia is widely used by companies to reach-out for customers. This approach is used in sale of groceries, household goods, electronics, clothes and other products through e-shops. Therefore, there were no urgency to transit business to e-commerce.

However, considering that consumer habits have changed due to closure of shops and shopping centres, now, more than ever before e-shops have become important places for processing personal data. In this regard, the main concern that merchants are facing is securing personal data of the users, including banking information. Experts point out that, in order to save resources and comply with security requirements, it is advisable to use already prepared e-shop platforms, which incorporate technical security solutions (HTTPS for communication, TSL, SSL - for data encryption, SET, CVV, AVS - for payment security, etc.).



COUNTRY SPECIFICS

Latvia – remote studying process

During the emergency situation, the study process was organised remotely in all educational institutions. Teachers were asked to assess and choose appropriate technological tools and working methods, in order to ensure a remote study process. In this regard, teachers were entitled to ask students to participate in video conferences, online webinars, receive photos or home-filmed videos for evaluation, etc. The Data State Inspectorate explained that it does not consider such teachers' approach to be inconsistent with the requirements of the GDPR, when the study process takes place remotely.

At the same time, the Data State Inspectorate noted that teachers should be assigning respective tasks to students in such a way that parents are duly informed about the curriculum and the need to send the relevant data to teachers. Also, in order to verify and examine the completion of the tasks assigned, teachers were instructed to choose learning methods impacting privacy to the least possible extent, for instance, use of applications, educational platforms, parental acknowledgment (in case a student does not have a smart device) instead of using web chats, videos, etc.

Link to the article »

Staņislavs Sviderskis
Lawyer

stanislavs.sviderskis@roedl.com
T +371 67 35 6392

Anna Kušnere
Lawyer
Certified Data Protection Specialist

anna.kusnere@roedl.com
T +371 67 33 8125

9. LITHUANIA

Vilnius


Vilnius

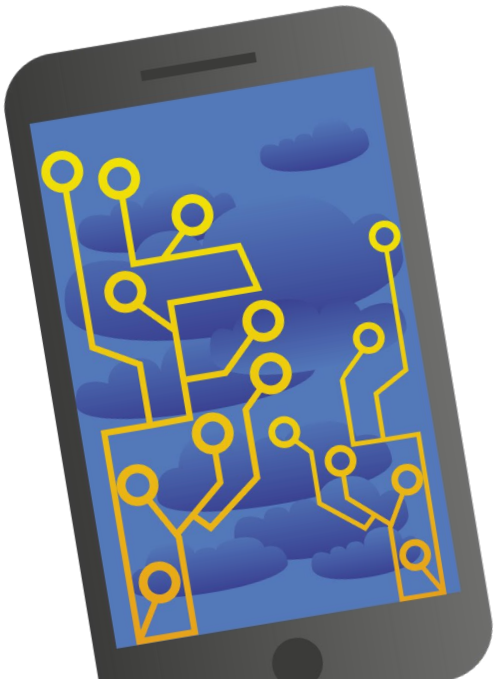
Processing of health data and geolocation

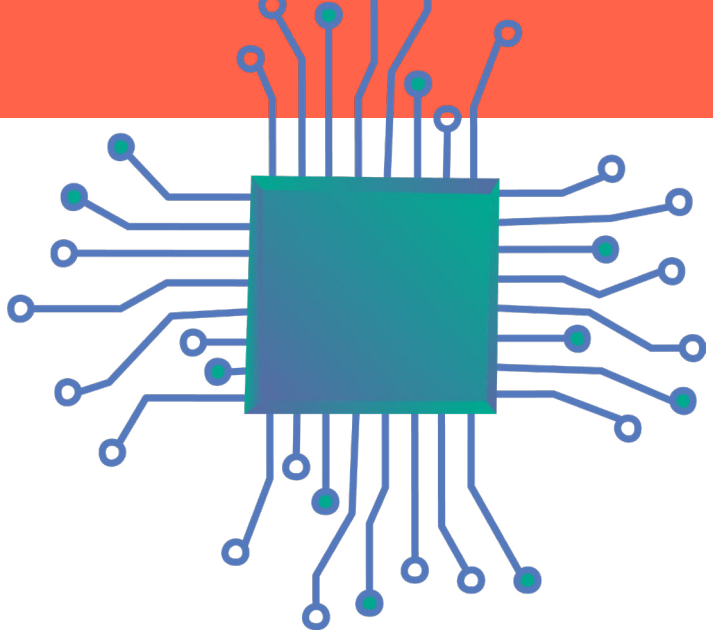
Authorities in relation to citizens:

- Technologies (termoscanner, drones, smart cities, thermal camera, swabs, sierological tests, medical certificate, etc.) and applications for contact tracing implemented in the respective countries / privacy by design, telecommunications' metadata (duly anonymised would be out of the scope of the GDPR but still requires security and confidentiality obligations), self-declaration models;
- Employer from its employees: return to the workplace, measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc. Attention on: Privacy statements, PIAs, risk assessments, data register, purpose limitation, integrity and confidentiality, proportionality and data minimisation, privacy statements, organisational and technical measures;

On 17 March 2020 Article 49 of the Labor Code of the Republic of Lithuania (hereinafter - the Labour Code) was amended as follows "when the Government of the Republic of Lithuania declares an emergency situation or quarantine in order to ensure the health protection of employees and third parties, the employer must offer in writing to work remotely to such employee whose health condition endangers the health of other employees. The employer's offer to the employee to work remotely must include the reason, time period and legal basis for such offer."

The Lithuanian State Data Protection Inspectorate has provided an explanation, that such provision essentially means, that if an employee has an illness that threatens to other employees health, such employee should inform the employer about the fact of such illness which endangers the health of other employees, but indicating only the fact of the illness or that there are circumstances that he might have been infected with such illness. Therefore, in order to comply with the principle of data minimisation, the employee provides to the employer only such information which would obligate the employer to enable the employee to work remotely. And the employer in the offer to work remotely should not indicate the certain employee's illness as the reason for remote work, but should choose instead a less intrusive reason for an employee's privacy, such as the health protection of other employees.





The Lithuanian State Data Protection Inspectorate also informs that employers may process certain personal data of employee's related to the current coronavirus (Covid-19) situation and that it is in compliance with the GDPR.

An employer has the right to ask it's employees or visitors whether they have symptoms of Covid-19 or have been diagnosed with Covid-19. This information is important for the employer in assessing whether additional protective measures are needed, such as requiring staff who have worked together or who have been in contact with a sick / symptomatic person to undergo quarantine, to provide with a possibility for remote work or a health check. However, it is to notice that the right of access to this information does not imply that employers can document the information received or compile relevant data files. Employers should also refrain from collection of temperature measurements and medical records of employees and visitors. This cannot be regarded as the employer's duty.

WHAT PERSONAL DATA CAN BE PROCESSED?

- Whether the employee was traveling to a „state of risk";
- Whether the employee was in contact with a person traveling to a „state of risk" or suffering from Covid-19;
- Whether the employee is at home due to quarantine (without giving a reason) and the quarantine period;
- Whether the employee is ill (without specifying a specific disease or other cause);
- Employers may also process personal data relating to the employee, such as the fact of remote work and other restrictions to the employee's work.

Provision of information to public authorities: Employers may provide information to public authorities if there is a clear basis for doing so. For example, for statistical purposes (in such case the provision of identification of a particular data subject must be avoided).

- Companies from their clients and visitors: temperature measurements, etc.
- Companies from their providers: measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc, organisational and technical security measures

Teleworking

Country specific guides to regulate teleworking:

- Update of risk analysis, privacy impact assessment, data register due to the teleworking situation: Smart working;
- Design of teleworking policies / policies on the use of tools and devices: annex to workers' contracts; flyer and procedure;
- Security measures on company's information systems and Cybersecurity measures (secure teleconferencing, arising awareness) relating to teleworking device: specific guidelines;
- Implementation of employee performance monitoring measures and related activities: assessment of the risks, PIA, duly inform, ROPA update;

The Lithuanian State Data Protection Inspectorate has issued the recommendation for the teleworking. If due to teleworking the employer collects more personal employee's data, then usual, he has to inform employees accordingly (transparency principle). If employer decides to monitor employees (to monitor e-mail correspondence, conversations, employee's actions while using the employer's PC or mobile device, etc.) the employer has to perform the PIA, to inform employees accordingly, to prepare necessary policies. It is recommended to establish and announce clear guidelines for teleworking. The employers are advised to evaluate and to designate particular allowed secure working tools, devices and systems (secure teleconferencing, connection to employers servers, etc.).

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

- Remotely handling and reporting of security breaches: specific communication channels for breaches or severe cases of security breaches in the different countries;
- Attendance of the rights requests should be especially observed. Added difficulties since there are fewer resources and possibly more attention is being given to other issues;
- Contracting with new providers, especially digital / cloud services and products, must involve privacy and security reviews.
- Constant changes and faster operations than usual cannot lead to the disregard of information obligations, PIA's, risk assessments, updating ROPA, etc.

Websites protection

Attention to those companies who have seen the urgent need to launch into e-commerce:

- Cyberattacks: web-specific security policies
- Adaptation of the legal texts required on a website, privacy policy, legal notice, cookies, T&C's, etc.

Country specifics:

- Italy: Local Laws relating to processing operations of employee's and provider's data: from smartworking up to apps, swabs, sierological tests, medical certificate; Local laws relating to Covid apps
- Spain: Observance of digital rights in times of Covid-19.

Link to the article »

Jūratė Masiulytė-Katakinė
Senior Associate
Attorney at Law

jurate.masiulyte@roedl.com
T +370 5 2123 590

10. ROMANIA

Bucharest

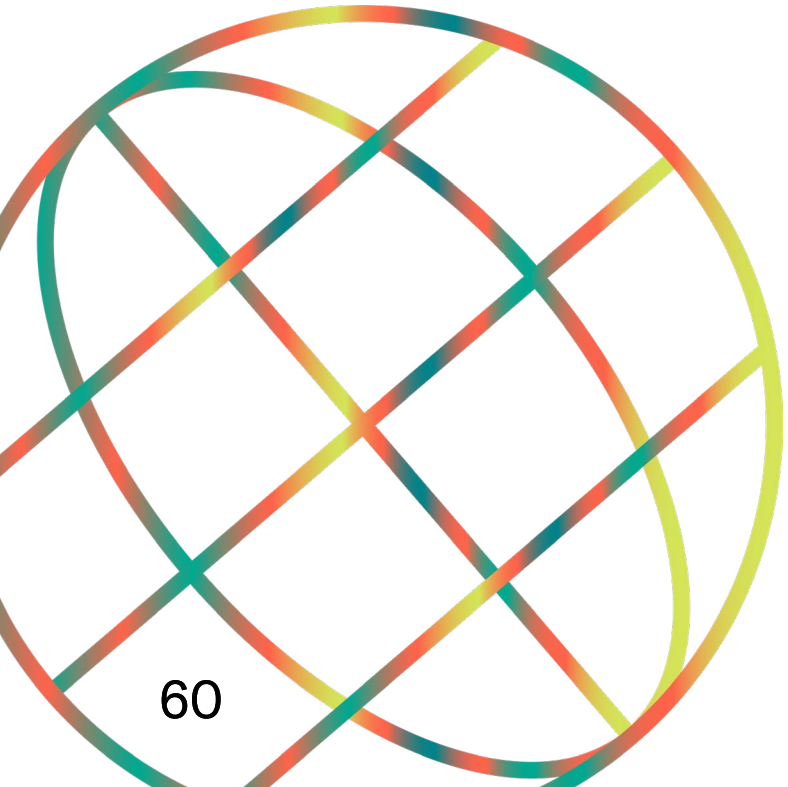

Cluj
Sibiu
Timișoara
Bucharest

Processing of health data and geolocation

Authorities in relation to citizens:

- (Termoscanner, drones, smart cities, thermal camera, swabs, sierological tests, medical certificate, etc.) and applications for contact tracing implemented in the respective countries / privacy by design, telecommunications' metadata (duly anonymised would be out of the scope of the GDPR but still requires security and confidentiality obligations), self-declaration models;
- Employer from its employees: return to the workplace, measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc. Attention on: Privacy statements, PIAs, risk assessments, data register, purpose limitation, integrity and confidentiality, proportionality and data minimisation, privacy statements, organisational and technical measures;
- Companies from their clients and visitors: temperature measurements, etc.
- Companies from their providers: measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc, organisational and technical security measures

As of 18 March 2020, the position of the Romanian Data Protection Authority on the matter of processing health related data is that there needs to be legitimate grounds for such data to be processed (e.g. the employer's obligation to safeguard the health and safety of their employees, complying with public health measures etc.). More precisely, it recommended that controllers consider Article 9 of the General Data Protection Regulation, which sets out the conditions for processing health data, including when the processing is necessary for the purpose of fulfilling the obligations and exercising specific rights of the controller or data subject in the context of employment. Moreover, the ANSPDCP outlined that, with regard to the obligation to inform data subjects on the processing of their health data, controllers must take appropriate measures to provide information referred to in Articles 13 and 14 of the GDPR, in a concise, transparent, intelligible and easily accessible form, using clear language. If an employer fails to implement appropriate measures then it will potentially leave itself exposed to being liable for failing to ensure health and safety at the workplace.



It also makes reference to https://edpb.europa.eu/news/news_ro

Any active collection of data (such as body temperature and information on travel patterns and possible encounters with infected persons) from employees / visitors entering the premises is permitted, provided that such collection of data relies on a valid condition under GDPR (art. 6 letter d. and art. 9 (2) letters b., h. and i.) and is limited to what is necessary (e.g. employer must not request information about the medical history of the data subject or any medical documentation).

Please note that (a) employees are under a general obligation to immediately inform the employer about any circumstances which they believe to be a danger for health and safety at the workplace (risk of / confirmed infection with Covid-19) and (b) employers are required to notify the medical authorities, namely the Public Health Directorate (DSP) in case of a confirmed infection with Covid-19 among its workforce.

As regards the use of existing technologies (smart phones) for tracing people who have tested positive for the coronavirus and their contacts as a tool for stopping the spread of the coronavirus, emergency legislation in this respect is possible, but any Member State, thus including Romania, that adopts such a measure must put adequate safeguards in place and give individuals the right to judicial recourse. However, presently we do not have knowledge of such systems.

The following recommendations can be made in the context:

- Information of the data subjects (as per art. 13 in the GDPR) – for both employees and visitors entering the facilities in respect of any assessment questionnaires or health checks (e.g. temperature screening of employees and visitors entering the premises);
- Avoid collecting or keeping excessive data, especially health data (e.g. no records from the thermal scanner reading should be stored or archived)
- Consider the potential involvement of a health care professional in carrying the health checks;
- Consider updating the company's prevention and protection plan.

The retention period for questionnaires or other related records shall be set on a case by case basis, by each data controller, provided data shall not be kept for longer than necessary considering the processing purpose for which the data was collected. We recommend no retention period if there is no suspicion of disease, in the other cases a few days, which is required for epidemiological investigations / communication with the Public Health Inspectorate (DSP).

As a general rule, since it is about sensitive data (health data), we need to avoid any public disclosures or making the identity of the infected person accessible to persons other than:
- The staff, on a need-to-know basis; a general statement in case of a confirmed infection with Covid-19 among the workforce (avoiding the disclosure of the employee's identity) can be considered at the workplace, if not susceptible of preventing the fight against diseases / spread of the disease. However, prevention and fight against the disease / its spread implies a obligation to investigate and identify all individuals who were in direct or indirect contact with the employee who is or may be infected with Covid-19;
- Processors authorised for and instructed by the company to the processing of personal data (e.g. security company managing the access to the premises) on the basis of pursuing the specific purpose;
- Reporting obligations under local laws and regulations to public authorities acting in their institutional capacity.

Teleworking

country specific guides to regulate teleworking:

- Update of risk analysis, privacy impact assessment, data register due to the teleworking situation: Smart working;
- Design of teleworking policies / policies on the use of tools and devices: annex to workers' contracts; flyer and procedure;
- Security measures on company's information systems and Cybersecurity measures (secure teleconferencing, arising awareness) relating to teleworking device: specific guidelines;
- Implementation of employee performance monitoring measures and related activities: assessment of the risks, PIA, duly inform, ROPA update;

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

- Remotely handling and reporting of security breaches: specific communication channels for breaches or severe cases of security breaches in the different countries;
- Attendance of the rights requests should be especially observed. Added difficulties since there are fewer resources and possibly more attention is being given to other issues;
- Contracting with new providers, especially digital / cloud services and products, must involve privacy and security reviews.
- Constant changes and faster operations than usual cannot lead to the disregard of information obligations, PIA's, risk assessments, updating ROPA, etc.

All obligations under privacy regulations should be complied with by controllers and processors alike (notification of data breaches, exercise of data subjects rights and implementing adequate technical and organisational measures for all processing activities in the Covid-19 context).In respect of investigations, Romanian Data Protection Authority (ANSPDCP) has not issued any statements related to suspension of its activities, therefore, we shall assume that investigation activities will continue, with certain limitations (limiting the presence of the investigation teams at the companies' premises, with an accent on requesting documents and information in electronic format, method that was otherwise previously used by the authority).

Websites protection

Attention to those companies who have seen the urgent need to launch into e-commerce:

- Cyberattacks: web-specific security policies
- Adaptation of the legal texts required on a website, privacy policy, legal notice, cookies, T&C's, etc.

Country specifics:

- Italy: Local Laws relating to processing operations of employee's and provider's data: from smartworking up to apps, swabs, sierological tests, medical certificate;
  Local laws relating to Covid apps
- Spain: Observance of digital rights in times of Covid-19.

Link to the article »

Iulia Rezeanu
Senior Associate
Attorney at Law

iulia.rezeanu@roedl.com
T +40 21 3102 162

11. RUSSIAN FEDERATION

Moscow


Saint Petersburg
Moscow

Processing of health data and geolocation

The Russian Ministry of Communications has developed a system for tracking one's contacts with coronavirus infection. The system is based on the mobile phone geolocation data and informs one about the necessity to get isolated in case of a contact with a patient. Regional authorities have been instructed to include the phone numbers of citizens found ill with Covid-19 in this system, without providing other personal data.

An electronic pass regime was introduced in some regions to reduce the number of people outdoors and thus the probability of getting infected. According to the decrees issued by the heads of these regions, the personal data required to be included in such passes will be deleted upon termination of the pandemic.

Geolocation data are taken from street cameras and traffic monitoring systems as well as transport maps for public transports.

Companies from their providers:

Measures required to monitor health data of employees allowed in each country include temperature measurements, swabs, serological tests, medical certificate, etc. as well as organisational and technical security measure.

Since 12 May, additional measures have been introduced in some regions of Russia, including Moscow, to prevent spread of coronavirus in workplaces. First of all, beginning on 12 May 2020, the employer must deny access to workplace to employees with the following diagnoses: obesity, diabetes, mellitus, Degree two hypertensive disease, chronic obstructive pulmonary disease, Degree two bronchial asthma.

The employer is obliged to take temperature readings of employees once every four hours. Another new obligation of the employer after 12 May 2020 is to get their employees tested for the new coronavirus infection (2019-nCoV). The official document states that these tests should be performed on at least ten per cent of the employees once in every 15 calendar days. The employer is also under an obligation to deliver blood samples of employees to be tested in a laboratory applying ELISA (enzyme-linked immunosorbent assay) method for the presence of the new coronavirus infection (2019-nCoV) and immunity thereto according to the procedure and within the term established by the Moscow Department of Health. According to the explanations provided by RosComNadzor, these responsibilities are in compliance with laws on personal data and the Labour Code of the Russian Federation.

Pursuant to Article 88 of the Russian Labour Code, the employer may not request information about the employee's state of health, excepting the data indicating that the employee is able to perform their job functions. The employee's consent to the examination and tests is not required because the measures to detect illness are relevant for determining whether the employee is able to perform their job functions.

– Companies from their customers and visitors: temperature measurements, etc.

Visitors who do not have an employment relationship with the entity are deemed to have expressed their consent to the gathering of information on their body temperature (without their identification by name) by means of their particular actions reflecting their intent to visit the entity. In this case the visitor will be referred to a medic for consultation in case of a high temperature reading.

Teleworking

Country specific guides to regulate teleworking:

Teleworking must be made possible by the employer on the basis of the regulations on handling of personal data in the company. It is also recommended to develop internal documents defining threats to safety of the personal data in order to limit use of personal computer services by employees. Constant changes and operations faster than usual should not lead to disregard of information-related obligations, PIA's, risk assessments, updating ROPA, etc.

Link to the article »

Tatiana Vukolova
Associate Partner

tatiana.vukolova@roedl.com
T +7 495 933 5120

12. SPAIN

Madrid


Barcelona
Madrid

Authorities in relation to citizens:

Technologies (termoscanner, drones, smart cities, thermal camera, swabs, sierological tests, medical certificate, etc.) and applications for contact tracing implemented in the respective countries / privacy by design, telecommunications' metadata (duly anonymised would be out of the scope of the GDPR but still requires security and confidentiality obligations), self-declaration models;

In Spain, the development of a national self-assessment trial application called Asistencia Covid 19 has been enabled which allows geolocation of the user for the sole purpose of verifying that he or she is in the region in which he or she declares to be. The application can only geolocate the user who voluntarily downloads it and it is available in six Spanish regions. However, it seems that Spain has opted for the model proposed from Europe that is less intrusive on the privacy of individuals, that is, the installation of an application on mobile devices that, through Bluetooth –not geolocation-, emits and observes anonymous identifiers that change periodically. When two mobiles have been in proximity for a certain period of time, both save the anonymous identifier issued by the other and, if a user tests positive in the Covid-19 test, it is possible to alert the mobiles that have been in contact, always preserving the privacy of the individuals. The adoption of these tools will depend on the decision of the health authorities based on the results of the pilot projects that may be launched in the coming weeks.

Furthermore, an analysis of the mobility of individuals was launched, through the crossing of data from mobile operators. The Spanish Data Protection Authority ("SDPA") has issued a report on the subject and states that it does not pose a greater threat to privacy than it did before the pandemic, i.e. there is always the possibility of incomplete anonymisation, lax outsourcing or a cyber-attack that would place the location of users' mobiles in the hands of a third party.

The SDPA in the aforementioned report outlines – together with the measures described- other technologies that are being used to fight Covid-19 or whose use is being assessed: geolocation in social networks; websites and chatbots for self-testing or appointment; voluntary infection information apps (citizen initiatives); immunity passports and infrared cameras.

– Employer from its employees

Return to the workplace, measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc. Attention on: Privacy statements, PIAs, risk assessments, data register, purpose limitation, integrity and confidentiality, proportionality and data minimisation, privacy statements, organisational and technical measures;

Many companies are already preparing the reopening of shops and workplaces, in accordance with the phased de-escalation plan approved by the Government. Now they are questioning whether they can adopt measures to prevent the spread of the virus, such as measuring the temperature of their employees or carrying out Covid-19 or serological tests. These measures undoubtedly involve the processing of personal data.

Regarding the temperature measurement, the SDPA questions its effectiveness as to preventing infection and states that this measure should only be applied in accordance with the criteria defined by the health authorities, -both in terms of its usefulness and proportionality- which will regulate the limits and specific guarantees for the processing of the personal data of those

concerned. In the labour field, as that of occupational risk prevention regulations, the taking of the temperature could be useful within the framework of a more extensive processing of which other verifications and additional guarantees are part, which, in any case, respect the rights and freedoms established in the RGPD. Taking into account the above, the legitimate basis that could justify such processing would be the obligation of employers to ensure the safety and health of workers in their service in work-related aspects, established in article 22 of the Occupational Risk Prevention Act. Neither consent nor legitimate interest can constitute the legal basis of the processing.

The SDPA has not yet made an express statement regarding the performance of Covid-19 or serological tests. Given the case, probably the legal basis referred to would apply to this processing.

There is therefore no answer applicable to all companies, each of which will have to assess the legitimacy of the measure in the light of its proportionality. The implementation of this measure must always be accompanied by compliance with applicable privacy regulations. In particular, the obligation to inform the worker (Article 13 GDPR) must be observed in all cases and, where appropriate, a prior report must be issued to the workers' representatives. Depending on the circumstances, a data protection impact assessment may be required.

– Companies from their clients and visitors: temperature measurements, etc.

The SDPA recommends the full compliance of the Healthcare Authorities recommendations as aforementioned. The temperature measurement could not be effective, because there are asymptomatic persons who do not have fever or could be the case that some persons have fever for other reasons, all of this could lead to cases of unjustified discrimination. That is why it is needed a common temperature level agreement at which a person is considered potentially sick of Covid-19. The SDPA recommends introducing proportionate measures, useful and non-intrusive, always in accordance with the criteria of the Health Authorities. Particularly, the SDPA stated that the health data cannot be spontaneously processed by any manager of a public place simply because he thinks it is the best for his customers or users. In these cases, it can be produced a risk of discrimination, stigmatisation and perhaps public dissemination of health data. All of this can be aggravated by the risk of leaks of sensitive information and conflict with those people who understand the measure as an attack on their rights. For now, the agreed official measures are, mainly, the safety distance of two meters and the limitation of capacity to the 30 per cent of the facilities.

– Companies from their providers

Measures that monitor health data of employees allowed in each country: temperature measurements, swabs, sierologists' test, medical certificate, etc, organisational and technical security measures.

Pan-European Covid-19 mobile application approach

Spain's approach to digital tools for infection prevention is in line with that of the European Commission and the European Data Protection Board, which advocate the implementation of a voluntary use model, compatible with the GDPR, focused on the protection of individuals' privacy and interoperable across borders. Spain highlighted the importance of finding a coordinated approach at European level for these applications that guarantees interoperability and allows for a joint approach to health emergencies. Therefore a national working group on mobile applications has been set up, mainly focused on interoperability protocols.

Update of risk analysis, privacy impact assessment, data register due to the teleworking situation: Smart working;

The SDPA stated that the measures and guarantees established in the defined policies have to be adopted on the basis of a risk analysis that evaluates the proportionality between the benefits to be obtained from remote access and the potential impact of compromising access to personal information. The resources that can be accessed should be limited based on the risk assessment representing a loss of the client device and the exposure or unauthorised access to the information handled. Companies should avoid using teleworking applications and solutions that do not offer guarantees and that may result in the exposure of personal data.

- Design of teleworking policies / policies on the use of tools and devices: annex to workers' contracts; flyer and procedure;

The SDPA has determined the content of the policies related to telework. They must determine, among others, which forms of remoted access and what type of devices are allowed, also the responsibilities and obligations assumed by employees. It is necessary to provide guides adapted to the training of employees and they must be informed of the main threats by which they may be affected and the possible consequences of those threats. If the employees do not comply with the guidelines they must know the consequences, both for data subjects and for themselves. These guidelines should identify a contact person for reporting incidents involving personal data and address the internal procedures for provisioning and auditing of remote access client devices, the procedures for managing and monitoring the infrastructure, the services provided by managers and how the policy is reviewed and updated to reflect the risks involved.

- Security measures on company's information systems and Cybersecurity measures (secure teleconferencing, arising awareness) relating to teleworking device: specific guidelines;
  Some organisations have published recommendations on how to make home office securely.
- SDPA has published a technical note with some recommendations to protect personal data in mobility and teleworking situations. This note is divided into advices directed to the Data Controller, and on the other hand advices directed to the personnel that is involved in data processing operations.
- The National Institute of Cibersecurity has published (INCIBE) some technical aspects which should be taken into account in order to protect the infrastructure.
- The National Cryptological Center (CN-CERT) has published a complete guide that includes all the different publications that this entity has made during the Covid-19 situation.

- Implementation of employee performance monitoring measures and related activities: assessment of the risks, PIA, duly inform, ROPA update;

To date, the SDPA has not issued specific guidelines governing the suitability of technologies for monitoring employees working remotely. However, any company that uses available or forthcoming technology to monitor its employees and control their working hours or performance must verify that there is a legitimate basis for the processing and comply with all other data protection obligations.

Data protection obligations

Any exceptions due to the emergency situation, to the obligation comply with GDPR and local laws? Or do all countries need to comply as always:

The SDPA agreed to apply the fundamental right to data protection in full and not to suspend it during the state of emergency.

- Remotely handling and reporting of security breaches: specific communication channels for breaches or severe cases of security breaches in the different countries;

The SDPA establishes that the suspension of administrative deadlines provided for in Royal Decree 463/2020, which declares the state of alarm, does not affect the obligation to notify security breaches that affect personal data, so that those responsible are obliged to notify them to the within 72 hours. The presentation of this notification will be made telematically through the electronic means made available by the SDPA, with the option of making an initial notification within the said period if all the necessary information on the breach is not available. Subsequently, when all the necessary information is available, the information may be extended by means of an additional notification.

- Attendance of the rights requests should be especially observed. Added difficulties since there are fewer resources and possibly more attention is being given to other issues;

This emergency situation has not meant the suspension of the time limits for responding to the exercise of the rights that the GDPR attribute to individuals, regardless of the private or public nature of the data controller before whom they are exercised.

However, the SDPA referred to the Article 12.3 of the GDPR which allows the response period of one month to be extended for a further two months, provided that the reason for the extension is given, for example, by describing how the activity of the controller is affected by the Covid-19 crisis. In such cases, if it is not feasible to notify the person concerned of the extension within one month due to the conditions arising from the crisis, this could be done through an automatic response to the receipt of a request to exercise rights.

Websites protection

CYBERATTACKS: WEB-SPECIFIC SECURITY POLICIES

The e-commerce uses the Internet to allow customers to buy without leaving home. Due to the actual Covid-19 situation, many companies have rushed to set up websites in order to continue providing their services online.
Some good practices that need to be taken into account when creating an e-commerce are:
HTTPS protocol that increases the security when the web page is used also for online payments.

Besides, other protocols such as SSL (Secure Socket Layer) certificate and SET (Secure Electronic Transaction) protocol are also advisable.

In order to make secure payments the protocols needed are CVV (Card Verification Value) and AVS (Address Verification System).

It is very important to have secure passwords for both the administrator and the users and even if the information is encrypted, best way to avoid exposing customer's sensitive information is not saving it. So no credit card information should be stored in the database.

- Adaptation of the legal texts required on a website, privacy policy, legal notice, cookies, T&C's, etc.

As the state of emergency does not suspend the right to data protection, the legal texts required on a website must comply with the applicable regulation.

Country specifics

Facial recognition and video surveillance in University exams.
The board of Governors of the Spanish Universities submitted a consultation to the SDPA about the legality of conducting exams through facial recognition systems. The SDPA replied stating that the processing of biometric data related to a constant (during the exam) identification of the data subject is considered a special category of personal data. This means that there are two possible legal basis to process sensitive data: consent or the "substantial" public interest (due to art. 9.2 g GDPR). The SDPA discards consent if it is the unique way to take the exam, as it is no freely given because of the intimidation that a data subject could suffer against a public authority. Nevertheless, if some alternative options are given to the data subject and they have no consequences and are equal (similar cost or difficulty), it is a possible way to address the exams. The other possibility is the declaration of the measure as "substantial" to the public interest. However, the SDPA discarded this option, as there is no law that enables this possibility.
The SDPA also received a consultation of the board relative to the use of CCTV to control students during the exams. This option was discarded as it is considered disproportionate and breaches the minimisation principle since there are higher privacy interests than mere student control.

Link to the article »

Ane Aretxabaleta
IT Auditor

ane.aretxabaleta@roedl.com
T +34 91 5359 977

Jorge Gonzalez
Associate

jorge.gonzalez@roedl.com
T +34 91 5359 977

Ana Victoria Martinez
Associate

anavictoria.martinez@roedl.com
T +34 91 5359 977

13. TURKEY

Istanbul


Istanbul
Izmir

The managing body of the Data Protection Authority of Turkey, Personal Data Protection Board, has made a thorough announcement on 27 March 2020 and on 9 April 2020 regarding the processing of personal data during Covid-19 Pandemic

General Information

The fundamental principles of processing personal data [(i) being lawful and fair, (ii) being accurate and up to date where necessary, (iii) being processed for specified, explicit and legitimate purposes, (iv) being relevant, limited and proportionate to the purposes for which they are processed, (v) being kept limited to the period stated in the related legislation or to the period for which they are processed] are fully in force during the times of pandemic, without any exceptions.

The obligations of the data controller such as conformity with the laws and regulation, obligation to inform the data subject, privacy, minimisation of personal data are also fully in force.

Processing Personal Data Concerning Health

Personal data concerning health that is considered a “Special Category” of personal data by means of Personal Data Protection Law and processing such health data is subject to the explicit consent of the data subject. Personal data concerning health may only be processed without such explicit consent by persons who assume the obligation or secrecy or authorised public institutions and organisations for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and nursing services, planning, management and financing of health-care services.

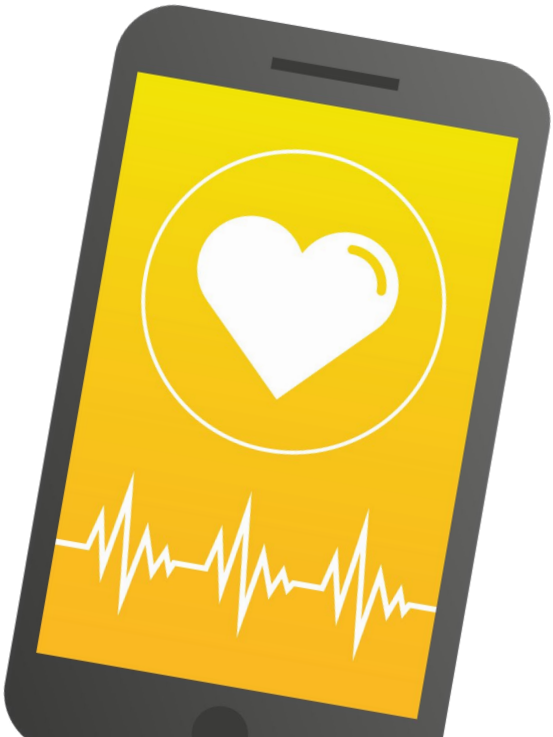
Accordingly, health data of the employees shall only be processed either by the explicit consent of the employee or without the necessity of the explicit consent, by the workplace physician or other health care personnel authorised by the workplace physician such as nurses, health officer, health and safety technical, who are all bound by the obligation of secrecy.

It is a fact that not many workplaces in Turkey have an assigned workplace physician. Therefore, explicit consent seems to be the most appropriate solution for the employer to process the health data of the employees. However, “explicit consent” of the employee is still a debatable concept, especially by means of labor law. Many argue that there is no explicit consent where there is an employment relation and thus the risk of losing a job. Furthermore, explicit consent may always be taken back, so the employer would then have to delete all the former health data that has been processed.

The employer, on the other hand, is obliged to keep the workplace and the employees healthy and safe. Therefore, Personal Data Protection Board has announced that the employer shall inform the employees of the infection cases. Such information shall not include the name of the infected employee as much as possible and only contain only enough data. In cases where the name of the employee shall also be disclosed, the infected employee shall be informed before such disclosure.

The announcement of the Personal Data Protection Board in fact conflicts with the Personal Data Protection Law, as the employer who has not engaged a workplace physician should not have access to and process such health data of the employee. We opine that Personal Data Protection Board made an exception to the law as the right of life supersedes the right of personal data protection. In any case, it is against the Personal Data Protection Law and an immediate amendment to the law is required urgently.

With this regard, the employer may take the fever of the employees at the workplace, may ask about the symptoms of fever or other virus related symptoms and / or the recent travel information of the employees as well as the visitors of the workplace. The employer may also disclose the health data of the employee to the authorised public institutions for the purposes of public health.



Is Location Data Considered Personal Data?

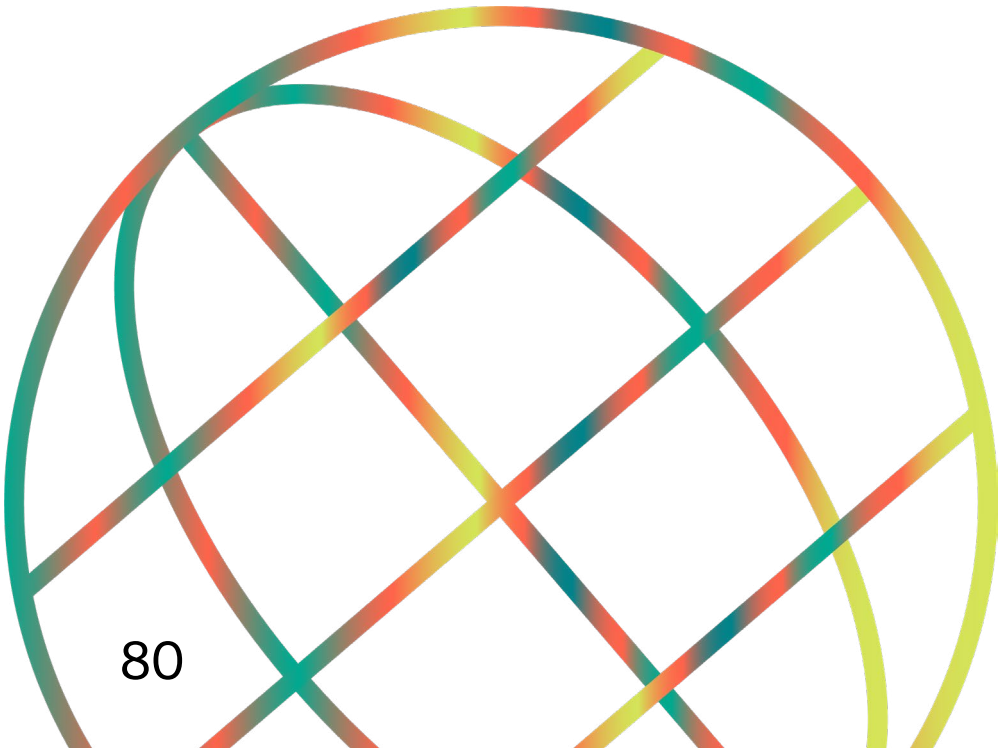
Personal Data Protection Law specifically states that in cases where the personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organisations duly authorised and assigned by law to maintain public safety and public order, the provisions of the law shall not be applied.

There are three conditions which are required to be fulfilled:

- Personal data should be processed to maintain public safety and public order,
- Personal data should be processed by public institutions and organisations duly authorised and assigned by law, and
- Personal data should be processed within the scope of preventive, protective and intelligence activities.

In cases where all three conditions are met, location data of persons may be processed by the authorised public institutions and organisations. Needless to say, authorised public institutions and organisations shall also take any and all technical and administrative measures in order to protect the safety of the personal data processed and also shall delete such data after the purposes of processing the same cease to exist.

However, any third party real or legal data controllers other than authorised public institutions and organisations shall not



Teleworking

During the times of Covid-19 pandemic, most workplaces adopted working home-office (remote working). Personal Data Protection Law does not hinder working home-office. The employees may work from home (or remotely from some other place) and even with their own devices.

However, it is very important that all technical and administrative measures are taken by the employee while processing personal data during working and also for the protection of the safety of the personal data processed. It is the obligation of the employer / data controller to inform the employees on the measures to be taken and also watch and observe whether such measures are adopted and applied.

Link to the article »

Ekin Dilek
Senior Associate,
Rechtsanwältin

ekin.dilek@roedl.com
T +90 212 3101 463

Serkan Özülkü
Partner
Rechtsanwalt

serkan.ozulku@roedl.com
T +90 212 3101 400

As attorneys, tax advisers, management and IT consultants and auditors, we are present with 109 own offices in 49 countries. Worldwide, our clients trust our 5,120 colleagues.

The history of Rödl & Partner goes back to its foundation as a solo practice in 1977 in Nuremberg. Our aspiration to be on hand wherever our internationally-active clients are led to the establishment of our first, own offices, commencing with Central and Eastern Europe in 1991. Alongside market entry in Asia in 1994, the opening of offices in further strategic locations followed, in Western and Northern Europe in 1998, USA in 2000, South America in 2005 and Africa in 2008.

Our success has always been based on the success of our German clients: Rödl & Partner is always there where its clients see the potential for their business engagement. Rather than create an artificial network of franchises or affiliates, we have chosen to set up our own offices and rely on close, multidisciplinary and cross-border collaboration among our colleagues. As a result, Rödl & Partner stands for international expertise from a single source.

Our conviction is driven by our entrepreneurial spirit that we share with many, but especially German family-owned companies. They appreciate personal service and value an advisor they see eye to eye with.

Our ‘one face to the client’ approach sets us apart from the rest. Our clients have a designated contact person who ensures that the complete range of Rödl & Partner services is optimally employed to the client’s benefit. The ‘caring partner’ is always close at hand; they identify the client’s needs and points to be resolved. The ‘caring partner’ is naturally also the main contact person in critical situations.

We also stand out through our corporate philosophy and client care, which is based on mutual trust and long-term orientation. We rely on renowned specialists who think in an interdisciplinary manner, since the needs and projects of our clients cannot be separated into individual professional disciplines. Our one-stop-shop concept is based on a balance of expertise across the individual service lines, combining them seamlessly in multidisciplinary teams.

WHAT SETS US APART

Rödl & Partner is not a collection of accountants, auditors, attorneys, management and tax consultants working in parallel. We work together, closely interlinked across all service lines. We think from a market perspective, from a client’s perspective, where a project team possesses all the capabilities to be successful and to realise the client’s goals.

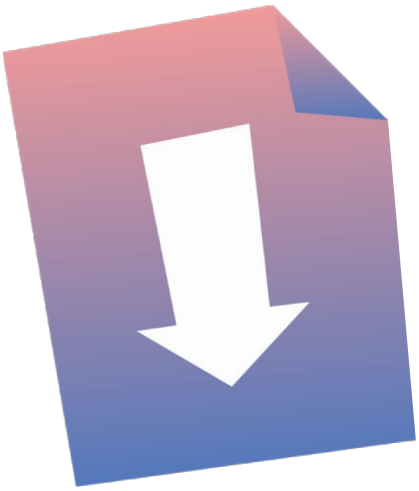
Our interdisciplinary approach is not unique, nor is our global reach or our particularly strong presence among family businesses. It is the combination that cannot be found anywhere else – a firm that is devoted to comprehensively supporting German businesses, wherever in the world they might be.

Data Protection Bites – Highlights from all over the world

The latest edition of our international newsletter is online, which aims at collecting all updates, news and insights on data protection issues, with particular attention to the GDPR.

Read more »

Subscribe for free »



RÖDL & PARTNER
Largo Donegani 2
20121 Milano

T +39 02 6328841
info@roedl.it

Visit us!
www.roedl.it