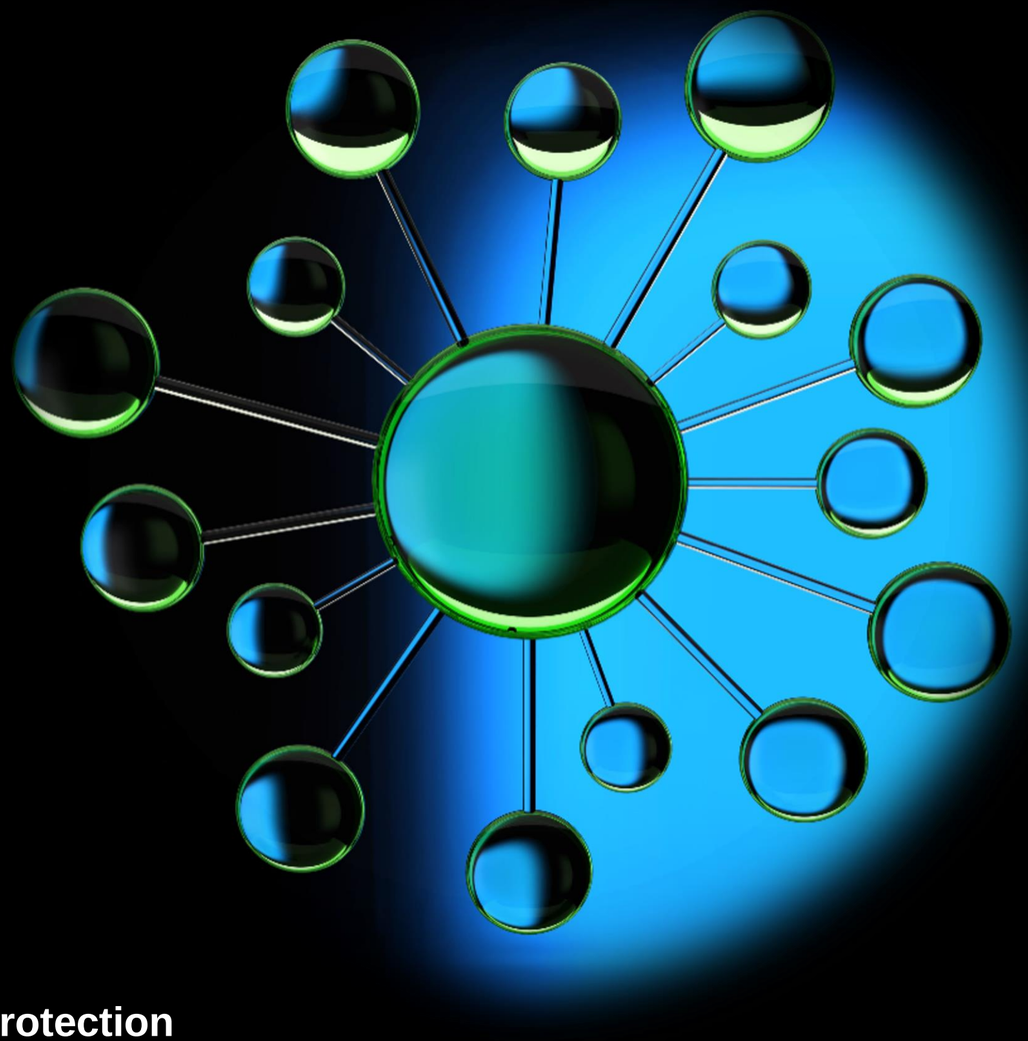
Deloitte.
Legal

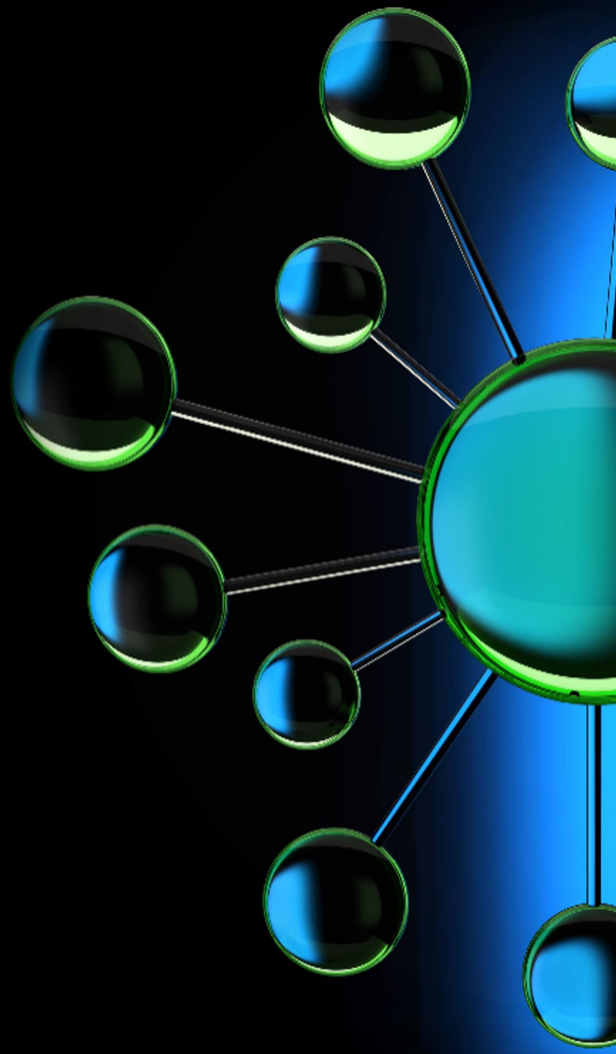


COVID-19 and European Data Protection

Booklet - III Release - Focus on Post confinement measures

June 22, 2020

Index



Introduction

Facing the public health emergency, the coronavirus pandemic, EAA countries prepared and implemented immediate measures in order to mitigate the social and economic impact of the outbreak.

Highlighting the most important questions concerning the lawfulness of data processing during the implementation of measures aimed to stop the spread of coronavirus, Deloitte examines the answers from each Member State.

The ***Deloitte COVID-19 and European Data Protection booklet*** is organized by FAQs and provides insightful, aggregated information about each European State, especially useful for **multinational companies**, that have to take into account national provisions.

New measures are implemented daily around the world. Therefore, please, consider the current version a thorough and accurate situation analysis at the publication date below.

Last updated: June 22, 2020

Does it make sense to talk about protecting privacy at a time when the general interest in fighting the pandemic is predominant?

*Not only it does make sense, but it is **essential** in order to enable preventive action to be directed **in the most balanced way and compatible with democratic principles**.*
*The challenge set by this health emergency is to combine effective action to prevent and combat contagion with the **essential guarantees of protection of fundamental rights**, such as indeed the right to privacy, which are subject to the **balancing test** with other legal principles such as, first and foremost, **public health**.*
*The rights might, in emergency contexts, be subject to even severe limitations, but such limitations must be **proportional to specific needs and limited in time**.*
***The strength of the democracy is also in its resilience**: in its ability **to modulate the exceptions** to the ordinary rules, according to necessity, setting them within a framework of certain guarantees and without letting go to improvisation*.

Antonello Soro
Chairman of the Italian Data Protection Supervisor
(Interview by Angela Majoli, Ansa, March 17, 2020)

Last updated: June 22, 2020

Post mandatory confinement period

Countries

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czechia
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovenia
- Spain
- Sweden
- Switzerland

Last updated: please, see indication for each Country

[19/05/2020] **last updated**

AUSTRIA

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Employers have a duty of care under labour law (both private and public) and must ensure that health risks at the workplace are excluded. For these reasons, the employer who wishes to protect his employees/customers from high-risk personal contacts may ask persons concerned about a possible stay in a risk area and about possible contact with infected persons / persons suspected of being infected. For suppliers, visitor lists (name and contact details) can be used to the extent necessary to inform visitors about an infection in the company (warning of a potential contact with an infected person has taken place). The data collected must be kept strictly confidential and may only be processed for the defined purpose. Whether the company might also take fever measurement is still unclear and depends on the individual case. As long as the fever measurement data is not stored (neither via thermal cameras, nor in the form of lists or with the help of applications), a measurement should be permissible under data protection law. It is also conceivable that suspected persons are questioned, but here too no storage in the form of questionnaires, records or lists should be made. For both measurements, particularly with regard to the principles relating to processing of personal data (Art. 5 GDPR), there is no reason for data processing or data storage after entrance or denial of entrance.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Employers are obliged (due to the duty of care in the employment relationship) to inform their employees about any Covid-19 infections that have occurred. In particular, in such a case, movement and contact profiles must be drawn up on the basis of the information provided by the infected person and other employees who have been in contact with the infected person must be informed of a possible contact. The name of the infected employee must never be mentioned to the other employees, customers or suppliers.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Such a measure, in the form of monitoring of employees and their contacts within the company, always depends on the individual case. In order to assess the admissibility of such a system, it is necessary to specify upfront whether the employer has access to this data (or can trace it back to the employee),where this data is stored and when the tracing app is active (working hours). If the employer does not have access to the stored contact data and the contact data is stored decentral (e.g. on the employee's device), such control may be permissible. It should be noted, however, that such a system requires the consent of the workers' council or - if no such council exists - the conclusion of an individual voluntary agreement (without coercion) with the employee. If the employer has access to this data and/or the tracing is outside working hours active such a processing is not permissible and generally also violates human dignity, so that it cannot be introduced or legitimize even by concluding a corresponding workers council agreement or an individual agreement.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	As with any new processing activity, the employer must base the processing on an adequate legal basis (Art 6 GDPR) and comply with data protection principles and obligations, in particular the company must update its processing register and employee information and assess the need for a DPIA and perform such if necessary. Employers should also ensure that relevant data erasure routines are taken into account in the design phase of the systems/ processing activities and that collected data is erased at the end of the COVID-19 pandemic.

[05/06/2020] **last updated**

BELGIUM (1/2)

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	In the event an employer takes the body temperature of a natural person prior to entering the employer's premises and requires them to provide certain information about themselves, this action shall most probably constitute processing of personal data, more specifically personal data concerning health. In such case, the GDPR will be applicable and the employer must comply with several requirements provided in the GDPR, this includes, without being limited to: transparency obligation, security obligation in respect of the personal data, verifying whether a data processing impact assessment is necessary and ensuring a legal basis for the processing activity. The legal basis for such processing activity is rather problematic. The processing of personal data concerning health is in principle prohibited, unless the employer can rely on one of the exceptions of article 9.2 GDPR. The relevant exceptions in this case could be: - Prior consent of the data subject: in order to rely on this exception, the data subject's consent must be freely given (cfr. consideration 42 GDPR). This shall e.g. not be the case when the visitor is not allowed to enter the premises when he refuses to give its consent. In the relationship between an employer and an employee, the "free" character of consent leads to additional concerns, as an employee is deemed to be in a 'dependency relationship' with its employer. The DPA states that the consent will in most cases not be a suitable legal basis. - Member State law: In Belgium, there is currently no specific legal provision upon which the employer can rely to process personal data concerning health. • Art. 20, 2° of the Law on employment contracts of 3 July 1978, which requires an employer to ensure that an employee can work in 'decent conditions', is not sufficiently specific to be considered an appropriate statutory exception to the processing prohibition in Article 9.1 GDPR. Neither is there a collective labor agreement in place. As there is currently no solid legal basis available, which enables the employer to process such personal data concerning health, the Belgian DPA asks the Belgian government to create a legal framework for body temperature measuring in the COVID-19 context.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	When processing personal data of an employee affected by COVID-19, it is in any case essential to take into account the basic principles of data processing. Additionally, the principle of confidentiality should also be taken into account. This implies that the employer may in principle not disclose the name of a COVID-19 infected employee amongst other employees. This could have a stigmatizing effect amongst other employees. With a view to preventing the further spreading of the virus, the employer is allowed to inform other employees of 'an infection' within the workforce, without revealing the identity of the person(s) involved. The name of the infected person may in any case be communicated to the occupational physician or the competent government services.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The Belgian Data Protection Authority (DPA) has not adopted any specific guidelines, recommendations or best practices in relation to the requirement of the employer towards employees to use tracing applications. On a more general note, and in the context of the review of two preliminary drafts of a Belgian Royal Decree in respect of the use of tracing apps, the DPA did state that every tracing application must comply with the rules, specifications and toolbox as set out by the EDPB (https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en). […]

[05/06/2020] **last updated**

BELGIUM (2/2)

➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	[…] For instance, the EDPB determined that the systematic and large monitoring of location and/or contacts can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all. It is also recommended to conduct a data processing impact assessment (DPIA) prior to launching the tracing application. In addition, it is noted that the principle of purpose limitation must be applied in order to exclude any further processing which is not related to the COVID-19 health crisis. Furthermore, it is noted that it is tracing applications can only be used to support manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Depending on the specific case and in addition to the required implementation measures stated in the previous questions (to the extent applicable), the employer should amongst others comply with the following: • Update the register of processing activities. • Comply with the information obligation (the EDPB emphasizes that in the event a tracing app is used, the controller should, in collaboration with public authorities, clearly and explicitly inform the data subjects about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app). • Implement technical and organizational measures (e.g. unique and pseudonymous identifiers generated by and specific to the application, state-of-the- art cryptographic techniques, etc.). • Maintain its retention policy: storage limitation should consider the true needs and medical relevance. Personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised. • Verify whether it should appoint a DPO (if it had not appointed it yet).

BULGARIA

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Bulgarian legislation and DPA have not explicitly addressed this question so far. However, employers are obliged not to allow employees and other persons with acute infectious diseases at the workplace. Therefore, they could process personal data, including health data (for symptoms of such diseases), for the purpose of performing this obligation. In any case, processing activities should be carried out in compliance with the principle of proportionality and data minimization.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Bulgarian legislation and DPA have not explicitly addressed this question so far. As part of their organizational measures with respect to the COVID-19 risk, employers in Bulgaria are instructed to establish an order to inform employees in case of a sick person with whom they have been in contact. However, considering the EDPB's recommendations, anonymized data should be communicated to employees, to the extent possible.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Bulgarian legislation and DPA have not explicitly addressed this question so far. In any case, processing activities should be carried out in compliance with the principle of proportionality and data minimization. Generally, undertaking such activities should be preceded by risk/ impact assessment, and the principles of privacy by design and by default should be considered as well.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Bulgarian legislation and DPA have not explicitly addressed this question so far. In principle, undertaking such new processing activities would require implementing various measures, among which: updating of the Record of processing activities; provision of information (privacy notices) to data subjects; undertaking appropriate technical and organizational security measures, etc.

CROATIA

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	No. If the employer suspects that the employee is affected by COVID-19 or that the employee has been in contact with the affected person, and consequently the employee starts showing COVID-19 symptoms (increased body temperature, cough, difficulty in breathing), the employer is obliged to inform its Safety at work expert or other authorized and qualified person for purposes of taking appropriate protection measures. The employee's body temperature could be measured by the employer only pursuant to the explicit employee's consent, provided it is compliant to the GDPR requirements.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Yes. However, such disclosure of an affected employee's personal data can occur only if ii) essential considering the respective employment environment (e.g. in case an affected employee works in the same working space with another employee) and (ii) such intervention over the employee's personal data and thus limitation of its personal private freedoms and rights is adequately proportional to the benefits resulting from such disclosure (e.g. disclosure at hand would eventually allow protection of another employee). The affected employee's data disclosed must be appropriate, relevant and limited to the purposes of data processing.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	No.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The employer must timely inform its employees on the terms and conditions of their data processing, and on its ability to protect their personal data. In case the employer intends to process special categories of personal data (such as personal data concerning employee's health status), it must ensure that such processing is performed in accordance with the GDPR requirements (e.g. the employer must obtain the employee's explicit consent prior to measuring employee's body temperature). Employer's Safety at work experts must pre-approve, arrange and subsequently scrutinize the employer's imposed measures.

CYPRUS

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Body temperature: An employer may take the body temperature of people entering its premises, provided it does so in compliance with the general principles of the GDPR, including having a legal basis for doing so. General Guidance to Businesses issued by the Ministry of Labour, Welfare and Social Insurance and the Ministry of Health states that the body temperature of personnel, customers, suppliers and/or visitors must be taken where such is considered necessarry, without, however, providing any examples. Provision of information as a condition to access the workplace: In accordance with the General Guidance to Businesses issued by the Ministry of Labour, Welfare and Social Insurance and the Ministry of Health, employees who experience symptoms of a respiratory infection or fever must not enter the workplace and must immediately inform their employer of such symptoms. Any other information collected from either the employees or other persons entering the workplace in connection to Covid-19 may be processed in compliance with the general provisions of the GDPR and employers may select to prohibit access if such is justified by the information provided by such persons.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The general principles of the GDPR must be adhered to when considering whether such disclosure is necessary. If, for example, the employer can find less intrusive ways of protecting the rest of the employees from any risk of infection, then the employer must opt for such less intrusive way of doing so. It should be noted that there is a requirement for the employer to notify employees of the location of the office of the carrier – where it is possible to do so without disclosing the identity of the employee, then such option is preferable.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	No express guidance has been issued in relation to this matter nor has it been expressly prohibited for employers to pursue such solutions. As such, employers must consider whether requiring employees to install or use such apps or other tools, is in line with the requirements of the GDPR, especially the principle of data minimisation.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	No express guidance has been issued in relation to this matter and as such the relevant obligations arising from the GDPR must be adhered to, including: • Providing the necessary notices (in accordance with Articles 13 and 14 of the GDPR) to the persons from which such personal data is collected; • Implement appropriate technical and organisational measures to ensure an adequate level of security of the relevant personal data; • Update the record of processing activities, where necessary; and • Carry out any necessary data protection impact assessments.

CZECHIA

[10/06/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	For the duration of the pandemic, which fundamentally endangers the health of employees and the public, the employers are permitted to ascertain the necessary information regarding the medical condition of the persons present in the workplace. In a situation where the employee refuses to undergo the examination or if his or her elevated temperature is measured, the employer can decide to deny the employee's access to the workplace or order the employee to stay home as prevention or, if necessary, to seek medical attention. However, the result of the temperature measurement does not have to be a sufficient basis to consider the employee unfit for work – if the employer measures an elevated temperature of an employee, the appropriate solution is a medical inspection of the employee. As regards other persons, the employers are generally not required by virtue of law to allow such persons to access the workplace in case of the measurement of elevated temperature. The appropriate solution will depend on contract terms with the supplier and/or individual circumstances. Always make sure that the measurement is performed by qualified experts.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The local DPA recommends not to disclose which particular person is infected, is in mandatory quarantine or whose elevated temperature has been measured, unless it is absolutely necessary. The employer should always, above all: Ensure that the dignity and integrity of that person are not affected; Inform the persons concerned in advance how their information will be treated and who they may contact; and Inform employees and business partners in advance about the measures taken.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The employer's ability to monitor employees' activities through tracing apps or other tools is subject to the rules of the protection of the privacy and personal data of employees. In this respect, the current pandemic does not bring about any relaxation of the rules. Thus, the employer would only be allowed to use the tools, as mentioned above, if a serious cause consisting in the employer's nature of activity existed.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Generally, all GDPR obligations addressed to a data controller, apply in case of any new processing – privacy by design should be observed (e.g. also by conducting DPIA and/or balancing tests), due performance of data subjects' rights must be ensured (including provision of specific Information notice) etc.

ESTONIA

[21/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	An employer does not have the right to measure an employee's body temperature (as well as health data) to find out if he or she has a fever. Unless agreed with employees and justified in an emergency to prevent COVID-19 infection when the employee comes into contact with other employees or customers. In case of emergency situation it may be justified to ask the employee for his or her health information if this is necessary to ensure the safety of other workers and / or customers., for instance, if the employee is working in food industry, healthcare organizations. The employer has the right to ask the employee if he / she has been in contact with people with COVID-19 infection. The employer also has the right to ask the employee for confirmation that the employee's state of health does not hinder the performance of work duties and is not a danger to other employees or customers.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Employers should inform other employees of COVID-19 incidents and take protective measures, but should not provide information about the identity of employee or provide more information than is necessary. The exceptions to the prohibition on disclosure of an affected employees name should apply only in very extreme and well-thought-out cases to a limited number of persons and only if disclosure of the name is strictly necessary to take precautionary measures.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Estonia laws implemented the ePrivacy Directive that states the principle that the location data can only be used when they are made anonymous, or with the consent of the individuals or its directly stated in the law. Using such devices, apps or other tools are allowed if it is recording information with the consent of the employee or if the employee performs the duties that requires collecting location data according to the law (for instance bus driver, taxi driver) . Processing location data outside the work-time is aloud only with the consent of the employee.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The employer must notify the employees about the additional measures that the employer plans to implement before employer started to implement new measures. If processing is based on consent, the employer shall be able to demonstrate that the empoyee has consented to processing of his or her personal data. Employer also has to amend a record of processing activities under its responsibility and internal documentation regarding possessing the personal data.

FINLAND

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	According to the Finnish Employment Data Protection Act, to perform inspections and tests on the health status of employees, only health care professionals, persons with relevant laboratory training and health care service providers can be used to conduct the same. The employer has a right to refer the employee to a health examination and use its direction right to determine place of work performance (with limitations). According to the Finnish Act on Occupational Safety and Health Enforcement, an OSH representative has the authority to suspend any work that causes immediate and serious danger. Suspicion of COVID-19 qualifies as a basis to request the employee not to access the premises. COVID-19 information is in general health data, and is not collectable as a condition for access to the workplace. Information on returning from a risk zone or being in quarantine (without specifying the reason) is not health data. Lawfully collected personal data based on an employee consent can be used to support OSH and direction right to determine place of work performance. Preventing other person's access to premises is discretionary, but may not be discriminating, and taking e.g. body temperature could only be based on a data subject consent.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	If an employee is diagnosed with COVID-19 or placed in quarantine, the employer may not, as a rule, name the employee in question. The employer can inform other employees of the infection or potential infection in general terms and instruct them to work from home. The employer is under an obligation of confidentiality concerning the health data of employees. If necessary, the employer can inform third parties in general terms and according to the organization's practices that the employee is prevented from carrying out the duties.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	According to the Finnish Employment Data Protection Act, the employer may only process personal data which are directly necessary for the employee's employment, which are related to the performance of the rights and obligations of the parties to the employment relationship or the benefits provided by the employer to the employees or are due to the specific nature of the work. The requirement of necessity cannot be waived with the consent of the employee. It is debatable, whether tracing of employees in order to control their movements and contacts within the company could be regarded as such basis, relating to e.g. occupational safety and health requirements, even considering the nature of the work and prevailing circumstances. In any event, if the necessity condition would be fulfilled, the Finnish Data Ombudsman has stated that tracing addressed directly to the employee e.g. by mobile phone, GPS location or other personal device, requires employee's consent. Further, location monitoring must be handled in the co-operation proceedings or, if not applicable, the employer must give employees or their representatives the opportunity to be heard on the above matters before taking a decision.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The GDPR principles and obligations for controllers and processors are applicable, including e.g. updating the record of processing activities, ensuring that data subjects can exercise their rights (such as access and rectification rights) and ensuring fair and transparent processing, such as defining data retention periods. Information must be provided to the data subjects in advance. As explained above, some lawful and necessary measures require also data subject consent. Technical surveillance, such as location monitoring, would require co-operation proceedings or, if not applicable, that the employer gives employees or their representatives the opportunity to be heard on the above matters before taking a decision. Following the co-operation or consultation procedure, the employer shall define the purpose and methods of the technical monitoring and inform the employees of the purpose, implementation and methods of the monitoring and use of data network.

FRANCE

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	From a French legal data protection perspective - except in specific cases as provided for in Article L. 1321-5 of the French Labor Code - employers are prohibited from: - **systematically processing** the body temperature of employees or visitors at the entrance of professional premises, **using** automated temperature sensors such as thermal imaging cameras, and recording the related information digitally or in a paper register; - However, please note that manual temperature measurements performed at the entrance of professional premises, without personal data processing and excluding any record of the related information, are not prohibited and may be performed by employers. In the meantime, please note that public authorities strongly recommend that citizens take their own body temperature in the event of fever or symptoms suggestive of COVID- 19. This does not prohibit requiring self-declaration on potential exposure to COVID-19 contagion prior to accessing the workplace premises.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	From a French legal data protection perspective, employers are prohibited from: - Reporting the identity of data subject(s) infected or likely to be infected by the virus to other employees (health privacy). However, this does not prevent employers from reporting cases of COVID-19 in the workplace to relevant health authorities. The French Data Authority (“CNIL”) has specifically stated that, where an employer is alerted to a case of COVID-19 among its employees, the employer may record: - the date and identity of the person suspected of having been exposed to the virus; - the organizational measures taken (isolation, remote working, contact with the occupational health physician, etc.).
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	From a French legal data protection perspective - and without any legal provision to the contrary being provided for with the adoption of the STOP-COVID app - employers are prohibited from: - Requiring of their employees that they install or use contact tracing apps or any other electronic or digital means, such as, for example, digital employee badges, that would enable employers to monitor their employees’ movements, location, and proximity to other staff at a particular work site or location;
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	In addition to the organizational measures mentioned above, employers may (legitimately): - remind employees working in contact with other people of their obligation to provide individual information to the employer or to the relevant health authorities in the event of any contamination or suspected contamination, for the sole purpose of enabling the employer to “adapt working conditions”; - facilitate the communication of such information by implementing, if necessary, dedicated and secure channels; - encourage methods of remote/tele-working and encourage consultations with occupational health physicians, if any; - inform employees by appropriate means (such as public notices or intranet) and the staff representative body (“comité social économique”), if any; - consult the staff representative body (“comité social économique”) if any, in the event of a major change in the organization of work (in accordance with Article L. 2312-8 of the French Labor Code) ; - provide prior, specific and appropriate information (including by means of training) concerning health measures, such as protective face mask(s), when required at the workplace(s).

GERMANY

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	In case of employees, § 26 III 1 Federal Data Protection Act (BDSG) is decisive. Therefore, such a measuring procedure is only permissible if it serves to fulfil obligations under labor law and if there are no interests of the employee that are worthy of protection. A mandatory temperature measurement would probably be inadmissible. However, voluntary fever measurements are possible. A declaration as to whether an employee was in a risk area or had direct contact with a sick person, e.g. questioning holiday returnees as to whether they had been in a risk area, should be allowed. However, general surveys of employees about travel destinations or their state of health are not permitted. The measurement of temperature in the case of visitors is not legitimated under Art. 9 Para. 2 GDPR. However, the query of general data (whereabouts, travel, etc.) is justified under Art. 6 Para. 1 lit. f GDPR, as there is currently an increased legitimate interest of the employer.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Under data protection law (Section 26 I BDSG/Art. 6 I 1 f GDPR/ Section 26 III BDSG/Art. 9 II b GDPR) collecting and processing of personal data (including health data) of employees is permissible in order to prevent or contain the spread of the virus among employees . This includes information in the cases, in which an infection has been detected or contact has been made with a person who is proven to be infected or in which a stay in an area classified as a risk area by the Robert Koch Institute (RKI) took place during the relevant period. The employer must inform his employees in case of a confirmed infection in order to identify and clarify possible contact persons as quickly as possible. However, the disclosure of personal data of persons who are infected for the purpose of informing contact persons is only lawful if knowledge of the identity is necessary for the preventive measures of the contact persons.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The currently planned tracing apps are based on the voluntary participation of the user. Employers could therefore encourage employees to use this app to protect themselves and others. However, they could not, for example, make its use a prerequisite for being allowed to enter company buildings. In particular, the obligatory introduction of such apps in the company can be considered a violation of data protection, especially against Section 26 I BDSG.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The responsibility for the implementation of necessary infection protection measures is borne by the employer according to the result of the risk assessment. The employer must seek advice from the occupational safety specialists and company doctors and coordinate with the Works Council. Specific measures according to the COVID-19 occupational safety standard (SARS-CoV-2-Arbeitsschutzstandard) : • Employees should keep a sufficient distance (at least 1.5 m) from other persons, • Further protective measures: partition walls, home office, working in small, fixed teams, mouth and nose protector, staggered working and break times, regular airing and personal use of work equipment, • Sufficient possibilities for hand hygiene, more frequent cleaning/disinfection of workplaces, • Transmission of current news to the employees; information on typical symptoms and the spread of the virus as well hygiene rules.

GREECE

[18/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	The Hellenic Data Protection Authority (HDPA) had received many queries from employers asking whether measures, such as taking the temperature of people entering their business premises, or asking employees to complete questionnaires about the health of their relatives or their travel history, or informing other employees about the identity of an employee infected by COVID-19, would be compliant with the GDPR. The HDPA has highlighted that: • All employers acting as data controllers should carry out all data processing activities that are necessary to ensure the protection of their employees' health, and none of the measures mentioned above could be considered automatically unlawful, especially during these unprecedented circumstances. • Any data processing should be carried out in accordance with Articles 5 and 6 of the GDPR, whereas employers are responsible for demonstrating compliance with the GDPR ("accountability principle"). • Employers should also make sure that they collect only data that is related to the processing purpose in accordance with the GDPR principles of purpose limitation and proportionality; • The confidentiality of the data collected should be protected through the requisite security measures. • With respect to more privacy-intrusive data processing (such as temperature controls at the entrance to facilities), these should be carried out only when there are no other less privacy-intrusive means to achieve the same purpose. • A systematic, constant and generalized collection of personal data leading to the creation and regular update of employee health profiles is highly unlikely to be compliant with the principle of proportionality.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The disclosure of personal data related to the health of the data subjects should not be permitted if it may lead to prejudice and stigmatization against the data subjects, and/or deter compliance with the measures imposed by the authorities, which may eventually undermine their effectiveness.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The HDPA Guidelines on processing of personal data for purposes related to COVID-19 do not cover in concreto the use of tracing apps or other tools in order to control employees' movements and contacts within the company. As per current HDPA doctrine the use of such mechanisms is restricted and not allowed if this could result in employees' performance systematic monitoring and assessment, in particular when less privacy – intrusive means can apply. Nevertheless, taking into consideration the unprecedented circumstances occurring due to Covid-19, employers could apply such data processing activities to the extent necessary to ensure the protection of their employees' health, as long as they are able to demonstrate that Articles 5 and 6 of the GDPR are well respected.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Pursuant to accountability principle, data controllers are required to put in place appropriate technical and organisational measures and be able to demonstrate their compliance with privacy legislation. Covid-19 does not differentiate this obligation with regard to the measures to be adopted. In this context, data controllers still will be required to apply privacy by design & by default principles, execute data protection impact assessments, update records of processing activities, draft tailor-made privacy notices, limit the amount of data processed etc. in order to demonstrate that the urgent and temporary measured adopted due to Covid-19 comply with GRPR requirements.

HUNGARY

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	The Hungarian Data Protection Authority regards disproportionate the requirement of screening tests with any diagnostic device (in particular, but not exclusively, with a thermometer) or the introduction of mandatory measurement of body temperature generally involving all employees called for by a measure of the employer, in view of the fact that the collection and evaluation of information related to the symptoms of coronavirus and drawing conclusions from them is the task of health care professionals and authorities. The employer and the physician providing health care carries primary responsibility for the compliance of data processing. If based on the report of an employee, or in an individual case upon consideration of all the circumstances, or on the basis of a risk assessment, the employer finds it absolutely necessary for certain jobs, particularly affected by exposure to the disease the employer may only call for tests to be carried out by health care professionals or under their professional responsibility and the employer is entitled to be informed only about the results of these examinations.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	No. It would not be proportionate to the rights of the data subjects. Nevertheless, with the view to the position taken by the Hungarian Data Protection Authority, it follows from the general requirements of conduct applicable to employers and persons in an employment relationship aimed at performing work, thus in particular, the obligation to cooperate and the principles of bona fide action and fairness that employees must inform the employer of any health or other risk affecting the workplace, other employees or third persons in contact with them in the course of performing work, including the risk of themselves being potentially infected.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Highly likely not. In the course of implementing enhanced control of persons entering the employer's site and restrictions related to this an action plan shall be elaborated, in which a particular attention should be paid to weighing the data protection risks of the measures applied in advance and to build efficient and adequate channels of communication to facilitate the provision of information to the data subjects. Detailed information and a notice has to be drafted and made available to employees and third persons, which contains the most important information related to the coronavirus (source of infection, mode of spreading, period of incubation, symptoms, prevention), together with an appeal addressed to them to immediately notify the access control staff about the fact of any presumed contact with the coronavirus or the onset of other conditions specified in the information material upon entering the site of the organisation.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Specific detailed information notice must be elaborated, as well as a necessity and proportionality test must be pursued. It is as well important to update the data processing activity record, pursue a data protection impact assessment, and prepare retention and deletion scheme of personal data. According to the Authorities standpoint, the employer can act in compliance with the law by applying the legal basis according to GDPR Article 6(1)f) or e) as well as the conditions set forth in GDPR Article 9(2)h) and (3). A DPIA would have to be pursued to analyze the exact circumstances of use.

IRELAND

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	The guidance from the Irish Data Protection Commission has not been updated since 6th March 2020. The guidance and the issues discussed therein remain relevant subsequent to any mandatory confinement period. 'Implementation of more stringent requirements, such as a questionnaires and temperature checks, would have to have a strong justification based on necessity and proportionality and on an assessment of risk. This should take into consideration specific organisational factors such as the travel activities of staff attached to their duties, the presence of vulnerable persons in the workplace, and any directions or guidance of the public health authorities.' In short, an employer must have a clear legal basis for collecting and processing the special category data referenced above, consideration of the other GDPR principles, including transparency, data security, minimisation etc. must also take place.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Identification of an individual infected by COVID-19 should be avoided in the interests of maintaining the confidentiality of the employee's personal data. The DPC advise that, an employer would be justified in informing staff that there has been a case, or suspected case, of COVID 19 in the organisation and requesting them to work from home. This communication should not name the affected individual.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The DPC has not specifically addressed this issue, however where an employer is considering the introduction of such new technology and are mandating its use, a DPIA will be required in line with Article 35 GDPR. It may prove very difficult for an employer to justify that such processing is 'necessary' given that the same data could arguably be collected using alternative mechanisms. Given that consent cannot be relied upon in the context of an employer/employee relationship, a detailed assessment of the legal basis relied upon should be evidenced in the DPIA including detail as to why the employer feels the legal basis relied upon adequately supports the mandatory use of such technology.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The DPC has been very clear in its guidance around transparency, 'Organisations processing personal data must be transparent regarding the measures they implement in this context, including the purpose of collecting the personal data and how long it will be retained for. They must provide individuals with information regarding the processing of their personal data in a format that is concise, easily accessible, easy to understand, and in clear and plain language.

[15/06/2020] **last updated**

ITALY (1/2)

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	In the light of the "Protocol for the regulation of measures to fight and contain the spread of the COVID-19 in working environments" signed by the Government and workers representatives on 14 March 2020 (as amended on 24 April 2020), employers can measure the body temperature to employees, customers, visitors and suppliers before they access the Company premises. In addition, among the measures to contain contagion, there is the prohibition to access the workplace applying to those who have been in contact with COVID-19-positive individuals over the past 14 days or come from risk areas according to WHO indications. To this end, a declaration regarding the above circumstances may be requested from employees and third parties such as visitors, suppliers etc. These activities shall be carried out in compliance with necessity and data minimization principles. For this purpose, it will be appropriate to measure the temperature without recording the collected data and without associating it with the Data Subject, unless it is necessary to document the reasons that prevented access to Company premises. In any case, only the necessary and relevant data will have to be collected without requesting additional information about the COVID-19-positive person and the specific places visited.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	With a view to the protection of the health of other workers, it is for the competent health authorities to inform the 'close contacts' of the diseased employee in order to implement the required prevention measures. Conversely, the employer is required to provide the competent institutions and health authorities with the necessary information so that they can carry out the tasks and duties set out also in the emergency legislation adopted in connection with the current outbreak. Data concerning health may only be disclosed, whether externally or within the organization an employee or collaborator pertains to, if this is provided for in the law or ordered by the competent authorities on the basis of statutory powers - for example, solely for the prevention of contagion from COVID-19 and upon a request by the health authority for tracing back the 'close contacts' of a worker who tested positive for COVID-19.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	No. By the Legislative Decree 30 April 2020 no. 28 , the Italian Government established the COVID-19 Alert System called "IMMUNI", which represents the national digital contact tracing system aimed at combating the spread of Covid-19 . This System includes a mobile APP, which is the only mobile APP authorized by the Government with the abovementioned Law. In addiction, the Italian Data Protection Authority with the Decision of 1 June has authorized the Ministry of Health (i.e. Data Controller) to carry out the data processing performed by means of the mobile APP. Based on the impact assessment provided by the Ministry, the processing of personal data within the framework of that system can be considered to be proportionate since measures have been put in place to adequately safeguard the rights and freedoms of data subjects by mitigating the risks possibly resulting from the processing. Taking into account the complexity of the alert system and the number of individuals potentially involved, the Italian Data Protection Authority considered it necessary anyhow to set out several measures in order to enhance security of the data related to the individuals downloading the mobile APP.

[15/06/2020] **last updated**

ITALY (2/2)

➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?

In order to carry out the processing activities related to the epidemiological emergency, employers are requested to implement technical and organizational measures appropriate to the risk related to new processing activties, in compliance with the GDPR. In addition, the organisational measures already in place should be extended to these processing activities such as:

- update the Record of processing activities, including the new processing activities;
- provide to employees, suppliers, visitors, customers a specific information notice, in all cases where a body temperature check is carried out and self declarations are collected;
- provide specific instructions to the persons authorized to measure the body temperature or to collect self-declaration;
- integrate pre-existing DPAs or draw up new DPAs to regulate relations with the Data Processors involved in the processing activities (e.g. security firm, where it is entrusted with the task of measuring body temperature).

LATVIA

[20/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	For prevention purposes, the employer may measure the temperature of employees and visitors who needs to enter the premises if the GDPR principles are in place. However, the employer cannot accumulate, compile, store the obtained data or otherwise use them thereafter. Also the employer can obtain information from the employees and visitors whether they have been abroad for the past 14 days and/or have they been in contact with COVID-19 sufferers or contacts.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The employer has the right to inform employees that Covid-19 has been diagnosed in the team without disclosing the employee's name (or other personally identifiable information) and to inform employees that they must comply with the safety and health measures for Covid-19 set by the responsible authorities.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The employer may track the employees within the company only in exceptional cases (for instance, if the employer is a medical institution) and if the GDPR principles are implemented in the company, as well if there is a clear and unambiguous justification for it and there is no other way how to achieve the aim. At national level an application is currently being developed in Latvia that can be used voluntarily by anyone to stop the spread of Covid-19. The application will inform all of those who have been in contact with an infected person without revealing their location (in the app contact will be defined as a 2-4 meter distance for longer than 15 minutes).
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Only if the employer has a clear and unambiguous justification for such processing, then the employer must implement appropriate technical and organizational security measures to protect the personal data as well as the employer must update its internal documents, privacy policies and inform employees of such processing.

LITHUANIA

[27/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	The employer as a data controller may take the body temperature, however, it should refrain from the storage of temperature readings of employees, customers, suppliers or visitors, medical records, or other data. Furthermore, the employer has a right to ask its employees or visitors whether they have symptoms of COVID-19 or whether they have been diagnosed with COVID-19, including this information: • Whether the person was traveling to a 'country of risk', • Whether the person was in contact with a person traveling to a 'country of risk' or suffering from COVID-19, • Whether the person is at home due to quarantine (without giving a reason) and the quarantine period, • Whether the person is ill (without specifying a specific disease or other reason).
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Only where a reasonable and objectively assessed basis exists (e. g. if non-disclosure would cause actual threat to health of other employees or similar). Otherwise, such information may not be disclosed as the rights and legitimate interests of affected persons have to be ensured.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The employer may not require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company. Such data processing would be considered as excessive and too intrusive with respect to employees' privacy.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The company should update the record of processing activities, evaluate the need for data protection impact assessment, establish the retention periods of newly collected data, ensure that the requirements with respect to special categories of personal data (such as access rights, storage security, etc.) are met, etc. Each company should review its internal policies and existing procedures and ensure that all actions as per those policies and procedures are taken with respect to the new data processing activities.

LUXEMBOURG

[15/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	No. Whilst the employer is responsible for health and safety at the workplace, the Luxembourg Data Protection Authority (CNPD) issued a recommendation stating that employers were not allowed to require their employees to disclose their body temperature. We consider that the same apply to any other third party. This also applies to self-declarations from the employees.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Such disclosure shall be considered as a processing of personal data that shall be governed at all times by the general principles provided for in the GDPR (such as, for example, the principles of minimisation or proportionality of personal data). In addition, the employer shall always ensure that the personal data of the employees are kept confidential. The employers may not disclose personal data of their employees to other workers or to third parties. However, based on their obligation to protect the employees' health and safety at workplace, the employers may need to exceptionally keep informed the colleagues of the infected employee, provided that such information is clearly justified. We advise to seek a prior legal advice before any disclosure of personal data.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Whilst the Labour Code allows employers to monitor their employees behaviour for the purpose of protecting the employees' health and safety, such monitoring shall abide at all times by the principles of the GDPR and be subject to the specific provisions provided for in the Labour Code. Based on our experience, the employer may only consider the use of tracking apps if it is reasonably justified.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	If a new category of personal data is processed by the employer, the latter shall update the record processing activities. At any times, the employer shall ensure that the processing is carried out in compliance with the GDPR and that the employees are duly informed of the processing. The employer shall also encourage the use of remote working and raise awareness of their employees regarding the risks related to Covid-19 and prevention measures.

MALTA

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	It is our understanding that, prior to admitting any person into the workplace, an employer should be permitted to administer body temperature checks, and to request information relating to that person's possible exposure to contagion including the collection of information such as recent social and/or travel history, and whether that person has had any recent contact with persons who are subject to self-isolation precautions. This data shall, in terms of Article 9 of the General Data Protection Regulation ("GDPR"), constitute a special category of personal data, and is subject to more stringent requirements of diligence when processing. Processing of this nature may be based on the employer's legal obligation to ensure the health and safety, at all times, of all persons who may be affected by the work being carried out for the employer, in terms of the Occupational Health and Safety Authority Act, Chapter 424 of the laws of Malta; without prejudice to any other lawful basis for processing in terms of Article 6 GDPR.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	An employer can, and should, inform employees that a fellow employee, or other person who may have been present in the workplace, has been infected with COVID-19. This information should also be provided to third parties who have been present at the workplace, or who have had direct contact with the infected person. However, the employer shall also be required to refrain from communicating any more information than shall be strictly necessary for the effective protection of the health of the relevant employees. It follows that the employees do not need to be informed of the identity of the infected person, except where this knowledge is absolutely critical for reasons which the employer becomes aware of. Where it becomes necessary to reveal the identity of the infected person, that person shall be informed in advance and measures shall be taken to ensure that their dignity and integrity is protected.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The measures which an employer may impose should adhere to the principle of proportionality enshrined within the GDPR. This means that the employer, as a data controller, is required to make all diligent effort to implement the solutions which are the least intrusive to the privacy of the relevant data subjects. Technologies such as tracing apps are generally viewed as being invasive, and should not be resorted to except in cases where a less intrusive option is not available or would not be sufficiently effective. Notwithstanding the above, an employer may require the installation of geolocation apps or other similar tools if this would appear to be the most legitimate and proportionate action available. However, the employer should first seek to process any data received in an anonymous way, which does not allow for the identification of individuals. Personal data protection rules shall not apply to data which has been appropriately and effectively anonymised.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	COVID-19 should not be viewed as a reason to weaken the principle that personal data should always be processed in a manner which is lawful, fair and transparent, particularly as many processing activities will apply to special categories of data. To the contrary, the good implementation of effective privacy policies and processes may complement the ability of employers to protect the safety of employees and other relevant persons. Among other things, companies should update their privacy policies and give their employees advance notice of how their personal data will be processed to deal with the COVID-19 pandemic. Data should be anonymised when possible and not used for any purposes which go beyond the purpose of collection. Data collected should be categorised and marked for deletion as soon as the relevant retention period has elapsed.

[19/05/2020] **last updated**

THE NETHERLANDS

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Taking body temperature: According to the Dutch Data Protection Authority, the GDPR does not apply to reading body temperature without storing or registering the data. However, the authority stresses that even though the GDPR does not apply, the processing can still impact the private life of the data subject. E.g. when a person cannot enter the office building after thermal screening and is being stopped in a row of people by a security guard, other people may draw conclusions from this action. Under strict conditions wherein the appropriate safeguards are in place, reading body temperature of people is allowed. Taking body temperature of employees can only be done by a physician, so not by the employer. Taking body temperature of customers, suppliers and visitors can only be done after obtaining explicit consent of the customer, supplier or visitor. Information on possible exposure: Employers are not allowed to process health data from employees for purposes not defined by law. Hence, employers cannot request information from employees on their possible expose to the contagion from COVID-19. Employers are allowed to request information on possible exposure from customers, suppliers and visitors.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	No. Following the strict interpretation of the law the employer is not allowed to ask whether the employee is tested positive for corona and process this information, and neither is the sharing of the identity of the infected employee with other workers. If the employee is tested positive (by a doctor), the doctor will inform the municipal health service (“GGD”) and the GGD Protocol will take effect. The GGD Protocol consists of a contact inquiry, including (if applicable) cooperation with the employer on how to inform employees who have worked closely with the infected employee.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	No. An employer cannot require employees to install and use tracing apps or other tools in order to control their movements and contacts within the company. This is only allowed under very specific circumstances. In general, this solution does not meet the requirements of proportionality and subsidiarity. Track & trace solutions are under heavy scrutiny, and are potentially only allowed if they are (inter alia) voluntary, anonymized and use decentralized storing of personal data.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Apart from general activities such as updating the record of processing activities and information notices, it is likely that the envisaged processing activities will trigger a required DPIA. Depending on the processing activity works councel involvement might also be required. In addition we recommend to draft a policy explaining the purpose and duration of the processing activity, the authorizations and security measures and how health data is processed (if any), by whom and under which conditions.

POLAND

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	As any processing of personal data, collecting information regarding body temperature of people requires identification of legal basis of processing. Under special provisions adopted due to COVID-19 outbreak, the Chief Sanitary Inspector acting under his authority may issue decisions imposing certain obligations on employers (and other legal entities or natural persons). As indicated in guidelines issued by Polish Personal Data Protection Supervisory Authority (PUODO) on 5 of May 2020, if the health inspector considers it necessary to adopt a solution in the form of measuring the temperature of employees and guests entering the premises of the workplace or obtaining statements from employees concerning their health condition, he may use a legal measure appropriate for him, as a result of which the employer will be obliged to measure the temperature or collect statements from employees concerning their health condition. The measures taken by the health inspector will constitute the legal basis for activities indicated in the appropriate decision, including the processing of personal data concerning health. In addition, in its guidelines PUODO also indicated that as regards measures against COVID-19 in the workplace, it should be noted that Article 9(2)(a) of the GDPR, i.e. the consent of the data subject, cannot constitute the basis for legalizing the processing of health data in the employment sector, i.e. in the employer-employee relationship and in the relationship with the public entity.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	When it comes to disclosing the identity of an employee affected by COVID-19 to other workers, the general GDPR requirements and labor law provisions will apply. Under Polish labor code, the employer is responsible for health and safety in the workplace and is also obliged, in case of any possible danger to health or life, to immediately inform employees about these dangers and undertake activities to ensure appropriate protection for them. Therefore, employers should inform employees about COVID-19 cases and take protective measures, but should not provide more information than necessary (i.e. if providing general information without indicating the identity of the person affected by COVID-19 is sufficient for preventive measures, the employer should not disclose such identity). In cases where it is necessary to disclose the name of an employee who is infected with the virus (e.g. in the context of prevention), the employees concerned should be informed in advance. Such information should be disclosed only to people whose security is in danger (and not to all employees). The employer must however ensure that the dignity of persons concerned is protected as well as all relevant GDPR principles are complied with. Since the disclosure of identity of an employee affected by COVID-19 to other employees is a sensitive issue and no common approach is adopted in this regard, the decision regarding disclosure should be made on case by case basis after a through analysis and only if there are no other measures to ensure employees safety.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	Since the Polish labor code provides only for the use of monitoring in the form of video surveillance and e-mail monitoring, it is not clear whether other forms of monitoring (for example tracing apps) are permitted and what are the conditions for their implementation. Therefore, such solutions should only be used after thorough analysis and only if they are necessary for ensuring safety in the workplace. In order to ensure compliance, it is also crucial to identify a proper legal basis for processing, in accordance with Article 6 of GDPR. However, in case the Chief Sanitary Inspector issues a decision imposing on employer the obligation to use tracing apps, such decision will constitute a legal basis for processing the data, as mentioned in the answer to the first question.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Each activity which involves processing of personal data, undertaken with regard to COVID-19 prevention, should be compliant with general GDPR provisions. Therefore, employer should in particular: define the specific purpose for processing personal data, identify appropriate basis for processing, ensure compliance with minimization principle, implement appropriate security measures, define retention periods, provide privacy notices to data subjects whose data are processed due to COVID-19 prevention measures, update records of processing activities.

PORTUGAL

[18/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	According to recommendation of the Portuguese Supervisory Authority (CNPD), employers may not collect and record the temperature of their employees or other health information or any potential risk behavior. Nevertheless, the Portuguese Government approved the Decree-Law no. 20/2020, of 01-05-2020, which authorizes the measurement of the employees' body temperature for the purpose of access and permanence in the workplace, forbidding, however, employers of keeping a record of it. When returning to the work premises, the collection of health data can be done by the employee by filling in questionnaires about health-related information or health-related private life data (e.g., if he/she has been in contact with people infected with the virus). However, it should be noted that the collection of health data is only legitimatized if it is carried out directly and exclusively by the occupational health professional.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Informing employees or others about the identity of any specific employee who is confirmed to have COVID-19 would involve disclosing special category personal data, and it is considered to be both unlawful from a data privacy perspective and employment law perspective. Depending on the case, there are several other less intrusive ways to address disease prevention, which would lead this practice to be considered disproportionate and unnecessary practice and therefore prohibited by GDPR and Portuguese national law. A balancing test is a relevant tool to assess this type of disclosure is possible under GDPR Article 9 exclusions either due to vital interests of data subjects or a public health interest.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The Portuguese Supervisory Authority (CNPD) refer to the EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Portuguese law do not address this particular subject, but It is understandable that depending on the application technical specifications, the information provided to data subjects and the data retention policy, the usage of tracing apps is possible as long as it is voluntary and not a requirement set by employers. The Directorate-General of Health (DGS) has developed a tool (Trace COVID-19) specifically for health professionals.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	As we are facing a new paradigm, several actions must be taken by Data Controllers in order to address its accountability regarding Data Protection. We have been advising our clients to update the Record of Processing Activities with the new processing activities, indicating specific data retention periods. We also advise to give detailed information to employees regarding temperature readings any other COVID-19 containment measure that may have impact on data subjects rights.

[19/05/2020] **last updated**

ROMANIA

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Yes. The Romanian legislation implementing measures to limit the spread of COVID-19 provides the obligation of employers to take the temperature of own personnel and of visitors, at the points of entry, and to prohibit access of persons with a body temperature exceeding 37.3 degrees Celsius and/ or with the symptoms of respiratory infection (coughing, sneezing, rhinorrhea, etc.) and/ or altered general state. The temperature may be taken whenever necessary during the work program. Employees which display during the working program respiratory infection symptoms and/or fever over 37.3 degrees Celsius and/ or general altered state shall be sent home/ to sanitary units, depending on the person's condition.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Not regulated expressly. In case less than 7 days passed from the moment when the COVID-19 infected/ suspected employee was on the company's premises, the Romanian legislation implementing measures to limit the spread of COVID-19 provides an obligation for employers to inform the persons with whom the confirmed/ suspected employee came into prolonged contact (more than 20 min, at a distance of less than 1.5 m and without wearing mask). The law does not specify that the contacts must be informed of the actual name of the COVID suspect/ infected person.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	The Romanian legislation implementing measures to limit the spread of COVID-19 does not provide for such measures.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The Romanian legislation implementing measures to limit the spread of COVID-19 does not provide specific data protection obligations associated to the measures to limit the spread of COVID-19. Also, the Romanian Data Protection Authority did not issue any new guideline in this matter. The general provisions of the GDPR shall be applicable in this context. Companies must: • Identify an applicable legal basis for the processing activity (most likely the applicable legal basis for health data shall be the one provided by art. 9(2) letter i) of the GDPR - processing is necessary for reasons of public interest in the area of public health on the basis of the national legislation). • Update their records of processing activities, as new processing activities shall be performed. • Adequately inform the data subjects (employees and visitors) with respect to the processing of their personal data. • Observe the principles set out in art. 5(1) of the GDPR when implementing the measures detailed above. For example, from this perspective, recording the temperature of all the tested employees in a registry kept for this purpose may be considered as excessive. Alternatively, the controller should consider recording the temperature of the employee only in cases where a significant decision is taken based on this information (e.g., the employee is denied access in the premises). • Implement adequate technical and organizational measures to ensure the safety of the personal data processed.

SLOVENIA

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Employers do not have a general authorization or requirement to measure the body temperature of employees/visitors. However, should the measurement of the body temperature or other information of employees/visitors be identified as reasonable and necessary to minimize the potential of contagion at the work place, such measurement can be applied. As per the opinion of the Slovenian Information Commissioner this is to be identified by the person authorized for occupational medicine, who should verify the necessity of measures in relation to specific circumstances (type/ nature of work, etc.) and if other less invasive measures may be even more effective in terms of actually preventing the spread of infection, e.g. to organize their work in such a way that a certain group of employees works a certain number of days, others remain in domestic isolation (thus the possibility of infection is significantly reduced). However, the consent of the person to obtain this data should be given. Should the respective person refuse the measurement/to provide information, the employer could deny entry to the premises of the company, in order to prevent contagion.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The employer must do everything possible to ensure that the identity of the sick employee is not disclosed. In case the employer is notified on the fact that the employee has tested positive, the employer shall collect information to identify persons who have been in contact with the employee and notify respective persons, but in principle on an anonymous basis. Namely, unless necessary, the employer should not disclose the name of the infected person (in accordance with the principle of confidentiality and the principle of data minimization) as this could lead to discrimination and stigmatization. If anonymity would not be possible, it is necessary to consider whether the duty to ensure safety and health at work and the protection of other employees prevails over the individual's right to the protection of personal data.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	In case of employer as data controller who is bound by the provisions of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No. 109/12 with amendments; ZEKom-1), special conditions and restrictions for processing of data on geolocations apply, provided by Article 152 of ZEKom-1, binding on the operators of electronic communications services. In the case the employer is not bound by Act or other special legislation, the decision on the legal basis for processing geolocation data must be taken by the controller in accordance with the provisions of the GDPR. In any case, the controller must respect the basic principles of personal data processing, including the principle of proportionality. Information Commissioner considered invasive measures such as “tracking” individuals for a specific purpose (i.e. processing historical non-anonymysed location data) as proportionate only in exceptional circumstances and if strong safeguards to secure the individual‘s rights are applied (proportionality of processing in relation to on the duration and scope, the limitation of the data retention period and the limitation of the purpose of the processing). Irrespective of the legal basis, the individual must be duly informed about the processing of personal data.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The company must ensure that persons are provided with transparent information regarding the collection of data, including the purpose of the processing and the retention period. In case of processing data, the consent of the person to obtain this data should be given. The company shall also adopt appropriate security measures and confidentiality policies to ensure that personal data are not disclosed to unauthorized persons (accessible only to certain persons and not for example the whole department). The Slovenian Information Commissioner expressed doubts about the necessity of continuous monitoring of employees and that, in the event of the planned introduction of such a measure, employers should carry out an impact assessment on the protection of personal data, which can be specific, short and concise.

SPAIN

[19/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	The Spanish Data Protection Agency (hereinafter, the "SDPA") provides for the possibility that security personnel may take the temperature of workers and suppliers at the time of access to the facilities, provided that it can be guaranteed that the data obtained from the temperature measurements strictly comply with the specific purpose of containing the spread of the virus, and not with other additional purposes, and that the data are not kept longer than necessary for the proper fulfilment of this purpose. Additionally, the request for information to employees and external visitors on symptoms or risk factors would be fully justified under the provisions of the applicable regulations on data protection and prevention of occupational risks. Such a request for information would not require the consent of the data subjects, even if it concerns special categories of data (health data), and the cooperation of employees and third parties in making this information available and its subsequent review may be a necessary condition to ensure their access to the Company's facilities in order to guarantee health protection.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	With regard to the information to be provided to the Company's personnel who may have been in close contact with the infected employee, the relevant information will be provided in accordance with the principles of purpose and proportionality set out in the applicable regulations. This necessarily implies that, as far as possible, this information should be provided without identifying the person concerned in order to maintain his/her privacy. However, it is envisaged that this information could be transmitted upon request by the competent authorities, in particular health authorities. Similarly, in the event that the objective of ensuring the health of other employees and society cannot be achieved with partial information, or the practice is discouraged by the competent authorities, in particular health authorities, identifying information could be provided to those employees who have had close contact with the infected person.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	In application of the provisions of the Spanish labour and occupational risk prevention regulations, employers may, in accordance with these regulations and with the guarantees established by these rules, process the data necessary to guarantee the health of all their personnel, and to avoid contagion within the company and/or work centres. However, personal data must continue to be processed in accordance with personal data protection regulations, as these rules have provided for this eventuality, and therefore their principles apply, including that of processing personal data lawfully, fairly and transparently, purpose limitation, accuracy and the principle of data minimisation. In addition, the SDPA has issued a document entitled "The use of technologies in the fight against COVID19. An analysis of costs and benefits", in which the benefits, risks and opportunities of different technologies are considered, such as apps for collecting information on infected people, contact tracking apps and digital immunity passports, among others.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	In relation to the new processing activities that will be carried out in order to guarantee the protection of the health of its employees and of third parties that may have access to its offices and facilities, the Company must update its record of data processing activities, inform the data subjects about these new data processing, and even update those risk analyses and privacy impact assessments. Beyond this, the Company, as the controller, may decide that certain activities are carried out in situations of employee mobility, or remote working. In this case, it is recommended that the Company adopts and defines a specific policy for mobility situations that takes into account the specific needs and particular risks introduced by access to corporate resources from spaces that are not under the control of the Company. This policy should determine which forms of remote access are permitted, what type of devices are valid for each form of access and the level of access permitted in accordance with the defined mobility profiles. It should also define the responsibilities and obligations assumed by employees, especially with regard to the guarantee and protection of personal data processed in the context of their daily activities.

[18/05/2020] **last updated**

SWITZERLAND

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	As the Swiss government has stated that there is no need for general COVID-19 testing for employees, the application of the principle of proportionality and data minimisation is particularly relevant here. When a private organization collects medical data from its employees (or visitors) before entering buildings, the processing must prove to be proportionate to the purpose of preventing infection and be limited to the necessary minimum. In particular with regard to its employees, it may be requested based on the employer's right for instructions, e.g. in case there were previous infections on the premises or if the premises is located in a high risk area. In such case, the employee is obliged to follow the employer's instructions and the data collection is permissible. In any other case, the decision of the persons concerned must be respected when collecting this data. There is no standardized guidance setting conditions for a justified intervention impacting on personal rights and it is advised to assess specifically the case at hand. Nonetheless, it should be borne in mind that we all have to be accountable for our actions and individually contribute to keeping our workplace and each other safe.
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	Employers must ensure the health and safety of their employees; it requires them to know about cases of COVID-19 in their organisations. Employers should also inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is appropriate to reveal the name of the employee who contracted COVID-19 (e.g. in a preventive context), the concerned employee shall be informed in advance and his/her dignity and integrity shall be protected and with securing his/her meaningful consent. Any disclosure of personal data or access to identifiable data connected with this case shell be restricted based on the need-to-know principle, and will be specific and proportionate with a view to preventing further contagions. If such sharing is pursuant to legal requirements, then the sharing should be strictly limited by the scope of the law.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	If the use of digital methods for the collection and analysis of mobility and proximity data is considered, employers must prove that it is proportionate to the purpose of preventing infection and provide a benefit which justifies the intervention into the personal rights. In general, the suitability of the tracing app for the office purpose can be questioned (and thus its proportionality). More appropriate seems to be introducing the measures and guidance based on the hygiene and social distancing guidelines by the Swiss Federal Office of Public Health, e.g. limiting building capacity and to create enough space for social distancing, increasing cleaning frequency and intensity of all office spaces and facilities, introducing a desk booking system. In a case of collecting personal data for public health purposes, the Swiss Federal Council, after consultation with the Data Protection and Information Commissioner, approved the public tests of the automated processing of sensitive personal data in the Swiss Proximity Tracing System as permissible under data protection law - further news here.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	Before implementing specific processing activities demanded by the current health protection measures, employers need to carefully consider the principles of purpose limitation, transparency, security and confidentiality, and accountability. Employers must be transparent about the reason for collecting data. This may be achieved by issuing clear, user-friendly and specific instructions to the employees and the issuing of data processing notices. It may be also necessary to obtain meaningful consent for some actions. Data should only be processed with the same methods as explained when employees are making the decision to participate. This collected data should be deleted when no longer useful for the declared purposes. An envisaged action will be updating or preparing records of processing activities. Also important is to provide appropriate safeguards to secure this data. Reliable security safeguards such as anonymisation, encryption, random identifiers or similar measures should be in place to protect people's data from unexpected exposure.

SWEDEN

[18/05/2020] **last updated**

➢ May an employer take the body temperature of people (employees, customer, suppliers, visitors, …) who need to enter the premises and require them to provide information, including through a self-declaration, on their possible exposure to the contagion from COVID-19 **as a condition for access to the workplace**?	Testing people who enter the premises is viewed as a significant integrity infringement. Which measures can be taken is a labor law issue and the possible examination types are dependent on the nature of the operations carried out at the workplace. For measures such as tests of employees entering the premises, the big difference is weather such tests are voluntary or not. Voluntary tests can be carried out easily, however if there is a collective agreement at place, the union must be notified prior to the initiation of tests. If the tests are involuntary, these will be harder to carry out, and an analysis of the importance of the tests versus the integrity infringement must be carried out. The type of business can have a great impact on this analysis (more likely to be granted at a health care provider).
➢ May an employer disclose the identity of an employee affected by COVID-19 to other workers?	The employer is obligated to take all necessary measures to ensure prevention of any diseases at the work place. Normally it should be possible to inform the employees without disclosing the identity of an affected employee. If the employer finds it to be absolutely necessary to disclose the identity of the affected employee, the identity can be disclosed once the employee has been informed about the disclosure.
➢ May an employer require employees to install or use tracing apps or other tools in order to control their movements and contacts within the company?	No. Installing applications for digital monitoring of a virus spread would require consent from each individual. Since consent is required, it is hard for employers to use such applications as employees normally are not able to give consent to their employers. Usage of such applications would also require that the integrity infringement is kept at the minimum. The gathered information may not be kept longer than necessary.
➢ What **measures** the company must implement as a consequence of such new processing activities of personal data (for instance updating of the Record of processing activities, specific instructions to the employees and information notice, …)?	The same measures as for all data processing activities are required. These measures include informing the employees and documentation of the processing activities as well as ensuring compliance, minimization of processing and protection of data etc.

Lockdown period

Countries

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czechia
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
The Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland

Last updated: please, see indication for each Country

AUSTRIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Employers have a duty of care under labour law (both private and public) and must ensure that health risks at the workplace are excluded. For these reasons, the employer who wishes to protect its employees from high-risk personal contacts may ask the persons concerned about a possible stay in a risk area and about possible contact with persons/persons suspected of being infected. Whether the employer might also take the employees' temperature is unclear, but may not be permitted since the above questions can be posed.

In order to prevent risks, it is also permissible for employers to request and temporarily store the private mobile phone number of employees in order to be able to warn them at short notice about an infection in the company or in the authority and so that they do not have to appear at the workplace. However, employees cannot be forced to make this announcement.

The employer may also use visitor lists (name and contact details of a visitor to a company) to the extent necessary to inform visitors of an infection in the company (warning that there has been potential contact with an infected person). The purpose of processing is to facilitate contact with visitors and to limit the spread of infection. The collected data must be treated in strict confidence and may only be processed for the defined purpose. In addition, access controls, i.e., fever measurement or visual checks for suspicious characteristics are also permitted. This does not affect the GDPR at all, if, for example, no data is collected when measuring fever, i.e., the values are not recorded.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The data protection law provides that these health data of the employees can be used to the extent necessary to contain the spread of the virus and to protect the fellow human beings. The employer is obliged (due to the duty of caare in the employment relationship) to inform his own employees about Covid-19 infections that have occurred in the company. In particular, in such a case, movement and contact profiles must be created to the best of the employer's knowledge and belief on the basis of the information provided by the infected person, and other employees who have thus been in contact with the infected person must be informed accordingly. The name of the infected employee must never be mentioned to the other employees. As mentioned before, it is also permissible for employers to request and temporarily store the private mobile phone number of employees in order to be able to warn them at short notice about an infection in the company or in the authority and so that they do not have to appear at the workplace.

In addition, at the request of the district administrative authority, employers who could contribute to the surveys are obliged to provide information about an infected person in accordance with § 5 (3) of the Epidemic Act 1950.

What to do if an employee shows symptoms of Coronavirus infection?

It is unclear exactly how the employer should proceed in a suspected case. Due to the duty of care under labour law, the employer should/must first of all send the person concerned home without delay.

Furthermore, if the contacts within the company can be traced, the employer must inform persons who have been in contact with the person concerned about the suspected case. However, no names may be mentioned. Furthermore, the employer should immediately vacate the work area and the department of the person concerned. The employer should have the possibly infected employee tested for COVID-19 or in any case ask him to do it himself. As stated above, employers who could contribute to the surveys are, at the request of the district administrative authority, obliged to provide information on an infected person in accordance with § 5 (3) of the Epidemic Act 1950.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

In the context of labour law, it should be noted that every employer has a duty of care towards its employees, which includes the exclusion of health risks at the workplace. Against this background, the processing of health data can be based on Art. 9 para. 2 lit.b GDPR in conjunction with the relevant provisions on the duty of care (processing for the purpose of fulfilling obligations under labour and social law). Data processing must be carried out in compliance with the purpose limitation principle in accordance with Art. 5 para. 1 lit.a GDPR. The use of health data for purposes other than health care, virus containment and curative treatment is therefore not permitted. After the end of the epidemic, therefore, that data which will no longer be necessary (such as in particular the private contact details of employees) must be deleted.

BELGIUM

[26/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

When processing personal data in the context of COVID-19 prevention measures, it is in any case essential to take into account the basic principles of data processing, such as determining the legal basis, observe the principles of proportionality, data minimisation, limited retention periods, meet the information obligation, and take necessary security measures.

It should be noted that, due to stringent confinement measures currently in force:

- remote working is currently mandatory for all non-essential businesses. Where certain functions cannot be performed remotely, work on company premises is permitted provided specific social distancing requirements are complied with.
- the above rules do not apply to essential businesses, although the latter are required to implement remote working and social distancing insofar as practically possible.

The above measures practically result in a drastic limitation of people currently accessing company premises. These measures are reassessed by authorities on a regular basis.

In case a company would want to have all visitors complete a questionnaire about medical data or recent travels, that would in any case not be allowed for employees. The Belgian Data Protection Authority rather suggests to encourage employees to spontaneously report risky journeys or symptoms to the employer. This is to be done in close collaboration with the occupational physician (‘médecin du travail’ - ‘arbeidsgeneesheer’).

In the opinion of the Belgian Data Protection Authority, checking the body temperature of a visitor does not per se qualify as processing of personal data, as long as such temperature information is not combined with other personal information. In practice, it will however be very difficult (if not impossible), not to do so, taking into account such measures as CCTV at the workplace, badging systems to access parking lots and company premises, etc.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The processing of personal data of an employee who tested positive for COVID-19 must in any case comply with the GDPR (see inter alia question 1), including the principles of confidentiality, data minimisation and proportionality.

This implies that the employer may in principle not disclose the name of a COVID-19 infected employee amongst other employees. This could have a stigmatizing effect.

With a view to preventing the further spreading of the virus, the employer is allowed to inform other employees of an infection within the workforce, without revealing the identity of the person(s) involved.

The name of the infected person may in any case be communicated to the occupational physician or the competent government services.

What to do if an employee shows symptoms of Coronavirus infection?

Employers have the obligation to take measures in order to ensure the safety of their personnel. However, it is the responsibility of the occupational physician (‘médecin du travail’ ‘arbeidsgeneesheer’) to monitor the health of employees whom the employer suspects were exposed to and/or show symptoms of COVID-19.

This results in the following obligations:

- As reminded by the Federal Public Service Employment, Labour and Social, in the event an employee becomes ill at work and is still able to return home independently, the employer must ask the employee to go home as soon as possible and to contact a doctor by telephone. It is advisable that the employee does not travel by public transport (unless there is no other option, in which case the employee must strictly apply the principles of sneezing and coughing hygiene during the ride home and wash his/her hands with soap and water before departure).

In the event the employee cannot return home independently, the employer (i) must call emergency services for urgent medical assistance or (ii) look for a solution in consultation with the employee’s family and/or his/her general practitioner.

- In order to prevent other employees from becoming infected, the employer should take adequate measures. Such measures can consist of isolating the infected person if he/she cannot go home immediately, giving the employee a mouth mask after washing or disinfecting his/her hands or let the employee cover his/her mouth, make the employee aware of the principles of sneezing, cough hygiene and let him/her wash his/her hands, disinfect all surfaces touched by the sick employee, etc.). Crucial in these circumstances is to consult with the employer’s occupational physician, so as to ensure that the measures taken are relevant and adequate.

In the event the personal data of an infected employee is processed, the processing activity must comply with the GDPR (see inter alia question 1 and 2 in this respect).

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing of the collected personal data is the prevention of COVID-19 contagion.

In order to be able to identify the legal basis that may be relied upon, a distinction is to be made between “ordinary” personal data and special categories of personal data (including data concerning health):

- For the first category, different options are available under article 6 GDPR. It is to be noted that the Belgian Data Protection Authority shared its opinion on the use of Article 6.1, d) GDPR (necessary in order to prevent vital interest). At this stage and based on the latest information published by the FPS Health (‘SPF Santé publique’ - ‘FOD Volksgezondheid’) on COVID-19, there is no reason for a systematic or more broad application of this legal basis by companies and employers, looking at implementing preventive measures.

- As far as personal data concerning health is concerned, specific grounds of article 9.2. must be relied upon. For employers’ articles 9.2. (i) (necessary for reasons of public interest in the area of public health) may at first sight seem relevant. However, the Belgian Data Protection authority clarified that this ground may only be relied upon in case employers act in accordance with explicit guidelines imposed by the competent authority. In this context, article 20, 2° of the Employment Contracts Act of July 3, 1978, may be of relevance. This article obliges the employer to ‘ensure that the work is carried out in decent conditions with regard to the health and safety of the employee’.

BULGARIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Bulgarian legislation and DPA have not explicitly addressed this question so far. There is a special order from the Minister of Health stating that: "All employers, depending on the specifics and capabilities of the respective work activity, should introduce a remote form of work for their employees.

Where this is not possible, employers shall arrange for enhanced anti-epidemic measures to be taken in the workplace, including: filter, disinfection and ventilation, personal hygiene instruction, and shall not allow employees or outsiders with acute infectious diseases". Considering that employers are obliged not to allow employees and other persons with acute infectious diseases at the workplace, they could process personal data, including health data (for symptoms of such diseases), for the purpose of performing this obligation.

In any case, processing activities should be carried out in compliance with the principle of proportionality and data minimisation.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

Bulgarian legislation and DPA have not explicitly addressed this question so far. According to the Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020 by the EDPB (the "Statement"), "Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary.

In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected."

As part of their organizational measures with respect to the COVID-19 risk, employers in Bulgaria are instructed to establish an order to inform employees, in case of a sick person with whom they have been in contact. However, considering the EDPB's Statement, anonymized data should be communicated to employees, to the extent possible.

What to do if an employee shows symptoms of Coronavirus infection?

An employee having symptoms of Coronavirus infection should contact his/her GP or call the national emergency number. Bulgarian legislation and DPA have not explicitly addressed employer's actions in this regard, apart from their obligation not to allow such employees at the workplace.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Bulgarian legislation and DPA have not explicitly addressed this question so far. The purpose of the processing can be defined as the prevention of COVID-19 contagion and protecting employees' health.

The legal basis could be legal obligation, when processing is necessary for compliance with a legal obligation to which the controller is subject. Where processing is not based on this ground, it may serve important grounds of public interest and the vital interests of the data subject, as outlined in recital 46 of the GDPR.

The retention period is not legally determined and should be set by the controller, e.g. with reference to the end of the state of emergency in Bulgaria.

CROATIA

[19/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

It is advisable for the Employer/Data Controller to adopt internal decision on processing of personal data of its employees and other persons occasionally entering its premises.

Pursuant to this internal decision prescribing these rules, the Employer/Data Controller should establish and predetermine its procedures of processing personal data and measures of personal data protection in the context of the COVID-19 outbreak (e.g. measure of measuring body temperature at the entrance of the Employer/Data Controller's premises).

The respective internal decision needs to be drafted and implemented pursuant to (i) the GDPR's principles of necessity of processing and data minimisation, and (ii) subject to the existing internal technical and organizational measures, as well as newly adopted (if necessary) in circumstances caused by COVID-19.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The Employer/Data Controller is authorized to process the affected employee's personal data, which may be necessary for compliance with the Employer/Data Controller's legal obligations related to health and safety at the workplace and/or the public interest (e.g. the control of diseases and/or other threats to health).

More specifically, the Employer/Data Controller would be authorized to conduct the internal investigations for purposes of identifying an employee potentially affected by COVID-19, and subsequently communicating the respective information on the employee's identity to the national health authority.

Within the procedure, the affected employee's personal data must not be disclosed to any third party outside of the state's police, national civil protection and/or health system, or other competent state authority.

The internal Employer/Data Controller's investigations need to be conducted in a manner which guarantees complete confidentiality and dignity of the affected employee.

What to do if an employee shows symptoms of Coronavirus infection?

The (potentially) affected employee is urged to inform the Employer/Data Controller on its symptoms so that the Employer/Data Controller is able to duly inform the competent health authority.

The affected employee, as well as all employees who were in direct contact with the affected employee, should be immediately isolated from their work environment and other employees.

The affected employee's personal data must not be disclosed to any third party nor should be made publicly available.

The protection procedures need to be conducted in a manner which ensures the confidentiality of all (potentially) affected persons.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Pursuant to the EDPB's recommendations resulting from the COVID-19 outbreak, the Employer/Data Controller would be authorized to process its employees' personal data when necessary for compliance with the Employer/Data Controller's legal obligations related to health and safety at the workplace and/or to the public interest (in this case particularly control of diseases and/or threat to health).

Additionally, special categories of data (in this case particularly health-related data) can be processed when in public health-interest (always pursuant to the data privacy EU law or national law), and for protecting the vital interests of data subjects.

The respective data's retention period should always be harmonized with the terms of the local law (when applicable), or other specific terms adopted during the state of emergency caused by the COVID-19.

CYPRUS

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

No guidelines and/or regulations have been issued in connection to privacy/data collection measures that need to be taken for people who need to enter the premises of the company, whether they are employees or visitors.

As such, the general principles of the GDPR must be adhered to (including, data minimisation, purpose limitation etc.) when processing personal data of employees and visitors in relation to COVID-19, also taking into account the provisions of the Health and Safety at Work Law of 1996 (L. 89(I)/1996) (the "Health and Safety Law"), which require the employer to ensure the health and safety of its employees at work (and any other persons that may be affected by the company's business), by inter alia:

a) providing them with such information and guidelines so as to ensure their health and safety at work;
b) providing and maintaining the workplace, including its entries and exits, in a condition which is secure and without health risks;
c) taking necessary measures for the health and safety of its employees and adapt such measures from time to time in accordance with the circumstances.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If an employee tests positive for COVID-19 whilst at the workplace, the employer must immediately inform the Ambulance Service providing the following information:

- Full name of the employee;
- Country of Origin;
- Symptoms of the employee; and
- Address of the working place.

All other employees must also be advised not to enter the employee's work location. Such notification should be made taking into account proportionality under the GDPR i.e. where employees are highly unlikely to have access to/enter the employee's office/place of work then they may not need to be notified of the fact that the particular employee has been diagnosed with COVID-19.

Once an employee tests positive, then all of the employees that have come into close or casual contact with the infected employee must be contacted in order to take the test as well – this is not however an obligation of the employer but of the Ministry of Health.

As such, any additional communication to employees must be carried out taking the general principles of the GDPR into account (and in particular confidentiality and proportionality), as no specific guidelines in relation to such communications have been issued.

What to do if an employee shows symptoms of Coronavirus infection?

Under the general obligations of an employee pursuant to the Health and Safety Law (i.e. to take reasonable care for his and others health and safety while at the workplace) , an employee must notify his employer of the fact that he has tested positive, in order to enable the employer to take the necessary measures to protect all other employees of the company.

The employee must also contact the Ambulance Service through the emergency number 1420 in order to inform them of his symptoms and help them determine whether a COVID-19 test is necessary. The employee must, irrespective of whether he is ultimately tested or not, place himself in self-isolation in order to contain the risk of contagion for a total period of two weeks.

As per above, any information provided to other employees in connection to the employee showing symptoms, must be made taking the general principles of the GDPR into account as no specific guidelines have been issued in relation to this.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

As per the below response, the purpose of the processing is the maintenance of the health of the employees and the prevention of the contagion of COVID-19 to other employees, contractors and/or visitors of the company. We consider the legal bases for this to be the following:

a) Where the personal data collected do not fall within the special categories, the processing can be based on Article 6(1)(c) i.e. compliance with a legal obligation (in this case, compliance with the Health and Safety Law) and on Article 6(1)(f) i.e. on the basis of the legitimate interests of the company provided that the processing (including the notification to other employees) is carried out in such a way so as to minimize the intrusion to privacy of the infected employee.

b) Where the personal data collected fall within the special categories, the processing can be based on Article 9(2)(b) i.e. that processing is necessary for carrying out the obligations of the controller in the field of employment insofar as it is authorized by Union or Member State Law – in this case, we consider the relevant law to be the Health and Safety Law as mentioned above.

As far as retention is concerned, no specific guidelines have been issued in connection to this and thus the general principle of retaining the data for as long as they are necessary for the purposes for which they were collected must be applied. Taking into account the sensitivity of the data in question, we would consider it appropriate for such data to be deleted once the health crisis has been surpassed.

CZECH REPUBLIC

[28/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Firstly, please note that there is no special regulation of this matter, which would be adopted in connection to C19 situation. Our answer is based on generally applicable employment, public health and data protection laws, respecting the current situation, where public health is at stake.

We believe that based on the employer's obligations in the area of Occupational Health and Safety, the employers are generally entitled to request relevant information from anyone who enters the premises of the company. This may include measuring body temperature or information about individual obligatory quarantine.

From the GDPR perspective, we believe that the processing of the information is based on legal titles under Art. 6 para. 1 letter c), or respectively under Art. 9 para. 2) letters b) and i) in case of health information. The processing principles mentioned by out Italian colleagues apply similarly.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The employer is entitled to process the data of the employee whose test is positive for infection solely to the extend necessary to ensure protection of health and safety of other employees, as referred to in our previous answer. The dignity and personal integrity of the concerned individual must be observed. The processing in this case, i.e. communication towards the employees who have worked closely with the infected employee, must comply with principles set by Art. 5 of the GDPR.

In our opinion and experience, the application of these rules has to be assessed case by case. Generally, it means that the employer will be allowed to reveal to its employees (at least some of them) the fact that another employee is diagnosed with COVID-19. The identity of such person is, on the other hand, barely necessary and thus the employer is not allowed to disclose it.

What to do if an employee shows symptoms of Coronavirus infection?

Please note that there is no special C19 regulation of this matter from the perspective of an employer. The employer does not possess any C19-specific rights towards the particular employee in this situation. Our answer is based on generally applicable employment, public health and data protection laws, respecting the current situation, where public health is at stake.

The employee that shows symptoms is generally recommended to contact his/her medical practitioner and/or the local Public Health Office.

From the employer's perspective – the employer should decide based on individual circumstances whether to let the employee stay at the workplace or order the employee to leave the workplace. Many legal and non-legal factors have to be considered by the employer. From the legal perspective, should the employer order the employee to leave the workplace, such situation would be considered as obstacles to work on the side of the employer and the employee is entitled to full remuneration.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing is identifiable in the prevention of COVID-19 infection and/or ensuring safety at workplace and public health.

As for the retention period, there are no specific rules set forth the by law, regulations or the local supervisory authority for this matter. Thus, only general principles, such storage limitation under Article 5 para 1 letter e), apply. Each company should evaluate the risks connected to both retention and deletion/destruction of the data at a particular moment. Generally, the retention period should reflect the termination date of the emergency state. However, there may be some high-risk individual cases where longer retention period can be legitimate, such as where disputes are at stake.

DENMARK

[01/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The employer may refuse admittance to the premises of the company.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If the processing of data is in compliance with the regulation on employment law, the employer is allowed to process data if the processing is in compliance with the current GDPR regulation.

Please note that the following are examples of information, which the employer may be allowed to process and address:

- that an employee has returned from a so-called "risk area“
- that an employee is in home quarantine (without stating the reason)
- that an employee is ill (without stating the reason)

What to do if an employee shows symptoms of Coronavirus infection?

See answer from no.2.

There is no specific legislation which allows/imposes the employer to take special measurements if an employee shows symptoms of Coronavirus infection

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

There is no specific prevention measure which applies to employers.

ESTONIA

[21/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The employer is able to ask the data about visiting the countries which are in the list and employee should provide information whether he or she visited foreign countries and contacted with infected people.

In a situation where the spread of an infectious disease is restricted, the employer must do everything possible to prevent the employees from coming to work.

Taking into account the specifics of the work, the employer shall compile an indicative list of health conditions which, in his or her opinion, could prove dangerous to the employee at work.

The employer must bear in mind that such an indicative list must not include health problems which do not actually affect the employee's ability to perform his or her duties.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

First of all, data about employee whose test is positive shall not be disclosed or communicated to third parties who are not the subjects.

The employer should inform other employees who have come into close contact with the positive subject and prevent from spreading to other employees.

What to do if an employee shows symptoms of Coronavirus infection?

In a situation where the spread of an infectious disease is restricted, the employer must do everything possible to prevent employees from coming to work.

Generally, in the context of today's situation, it is probably reasonable for an employer to ask the employee for confirmation that the employee does not pose a risk to other workers and the working environment in general.

Otherwise, the employer would not be able to fulfill its statutory obligation to provide a safe working environment.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Personal data shall be kept for no longer than is necessary for the purposes for which the personal data is processed.

FINLAND 1/2

[06/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Employer's direction, subject to certain exceptions, provides the employers a possibility to determine where the employees shall perform their work duties. There are certain formalities (codetermination obligations) for employers to follow. However, in this exceptional situation where the Government recommends all Finns to stay at their home and to avoid any transfers from one place to another, it is also easier for the employers to ask their employees to work from home on temporary basis. The fastest and easiest way is to implement remote/home working on voluntary basis (referring e.g. to Governmental recommendations and work health and safety issues, etc.) and agree on remote/teleworking rules and principles accordingly. However, in case company has employee representative(s) and/or work health and safety delegates elected in Finland, it is recommended to involve them into the process as well (in advance).

Actual measures are limited, if there is a need for entering the premises of the company. The companies (employer/data controller) are not entitled to conduct themselves testing or measuring body temperatures of their employees or third parties, such as suppliers. Employer's direction is mainly on determining the place where the employees shall perform their work duties.

Workplaces should update their hazard analysis and risk assessment in the light of the coronavirus epidemic.

The employer should draw up the necessary instructions and procedures regarding the coronavirus situation.

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If an employee is diagnosed with COVID-19, the employer may not, as a rule, name the employee in question. The employer can inform other employees of the infection or potential infection in general terms and instruct them to work from home. COVID-19 pandemic has not changed the rules on when and how the employer is permitted to process data concerning the employee's state of health.

The employer is permitted to process data concerning the employee's state of health (e.g. diagnoses) if the processing is required for the payment of the wages for the period of illness or other, corresponding health-related benefits or to determine whether the employee has a justified reason for absence. The processing of data concerning the state of health is also permitted if the employee specifically requests that his or her ability to work should be reviewed on the basis of the data. The employer is under an obligation of confidentiality concerning the health data of employees. If necessary, the employer can inform third parties in general terms and according to the organization's practices that the employee is prevented from carrying out their duties. If an employee is diagnosed with COVID-19 or placed in quarantine, the employer may not, as a rule, name the employee in question.

The employer can collect data concerning the employee's state of health from the employee. The collection of such data from other sources requires the employee's written consent. If the employee delivers a medical certificate or statement on his or her ability to work to the employer, the employer may deliver it to the occupational health care provider unless prohibited by the employee.

[…]

What to do if an employee shows symptoms of Coronavirus infection?

In general, the employer has a right to refer the employee to a health examination, but due to the nature of the COVID-19 pandemic, there are new guidelines (see below). An occupational safety and health representative (OSH) of the company can, under certain conditions, order an employee suffering from symptoms of a flu to go home. A shop steward cannot actually order sick employees to go home, but he/she can, of course, urge them to do so, as can other workers in the workplace.

As a guideline in the current epidemic situation, a symptomatic person is not allowed to go to work, even if the symptoms are minor. According to the Act on Occupational Safety and Health Enforcement, an OSH representative has the authority to suspend any work that causes immediate and serious danger. This may be the case if the symptoms clearly indicate a coronavirus infection and if the person works in contact with other employees. The OSH representative shall notify the employer of the suspension of work.

The sick employee shall be advised to leave the workplace and contact the occupational or public health care.

With a suspected coronavirus infection, one shall not go directly to doctor. A shop steward does not have a similar statutory right to suspend work, but of course in this situation, it is a good idea for anyone to encourage a coworker with flu to go home.

According to the Occupational Safety and Health Act, employees also in turn have a right to refuse work that puts their or someone else's life or health at risk.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

If personal data is processed at the workplace in relation to COVID-19, the employer is required to follow the laws applying to such processing. Health data belongs to the special categories of personal data that require specific protection. Health data refers to information about an individual's health, diseases, disability or treatment.

- The information that an employee has contracted Coronavirus is health data.
- The information that an employee has returned from a risk zone is not health data.
- The information that an employee is in quarantine (without specifying the reason) is not health data.

All of the above-mentioned information is personal data, however, and data protection legislation thus applies to its processing. In addition to the EU's General Data Protection Regulation (GDPR), the processing of employees' personal data is subject to the Act on the Protection of Privacy in Working Life. The Act on the Protection of Privacy in Working Life specifically provides for the processing of health data and stipulates that the personal data of employees may only be processed when necessary. The Contagious Diseases Act and other legislation related to occupational safety may also apply.

The retention period can be set – if applicable – with reference to the end of the state of emergency, i.e. as long as the information is necessary for the purpose it has been collected.

FINLAND 2/2

[06/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[…]

More information on what to consider in the risk assessment during the Corona situation can be found in the guide for workplaces provided by the Ministry for Social Affairs and Health.

The employer shall take care of occupational safety also in exceptional circumstances. In the coronavirus situation, the primary measure to prevent worker exposures is to avoid human contact. The employer shall assess the need for workers to arrive at the workplace from the point of view of the workers' health. One way to avoid contact is to work remotely; if it is impossible, the workplace conditions shall be organized to minimize the risk of exposure. These measures may include enhanced cleaning, hygiene instructions for employees, use of protective screens to prevent drip infections, guidelines for workers to avoid exposure to corona, and advice on situations where exposure or illness is suspected, and various shift arrangements. Another recommended measure is to avoid unnecessary gatherings in breakrooms in the workplace. If there is a significantly increased risk of infection, for example in work involving continuous human contact, personal protective equipment such as breathing protection, gloves, goggles and, if necessary, protective clothing shall be used.

Maintenance, cleaning, and replacement of personal protective equipment must be maintained at all times.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

[…]

The employer should keep documents containing data concerning the employee’s state of health separate from the employee’s other personal data. Neither may entries concerning state of health be saved in other personal data files maintained by the employer, such as payroll administration files. The employer and any personnel processing data concerning state of health on behalf of the employer are subject to a non-disclosure obligation and may not disclose the employee’s health data to third parties.

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Please note that the Office of the Data Protection Ombudsman in Finland has e.g. compiled answers (in English, too) to the most common questions concerning data protection and the coronavirus epidemic. Further, e.g. The Occupational Safety and Health Administration in Finland has also provided QA on their website.

FRANCE 1/2

[04/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Businesses and administrations may need to establish a "business continuity plan" (BCP), which aims to maintain the organization's essential activity. This plan must, in particular, include all measures to protect the safety of employees, identify the essential activities to be maintained and also identify the people necessary for continuity of service.
Employers have a general legal safety obligation of employers with respect to their employees. As such, it takes necessary prevention measures to avoid placing employees at risk. However, employers don't have an obligation to guarantee a zero-risk environment.

The employer has three types of action to initiate:

- Prevention measures: Providing employees with personal protective equipment (PPE) (e.g. sanitary masks, especially for employees in contact with the public);
- Information and training: Remind employees of "barrier" gestures to avoid the spread of the coronavirus (coughing into one's elbow, hand-washing, using disposable tissues, refrain from shaking hands, keeping one's distance),
- Changing the way work is organized in a manner appropriate to the situation: Reliance on teleworking where possible, adjust working hours, restrict access to premises or prohibit business travel in certain cases.

More specifically, we encourage you to follow the French National Research and Safety Institute for the Prevention of Occupational Accidents and Diseases (INRS)'s recommendations set out below.

Telework should be the rule for all positions that allow it. For jobs not eligible for telework and for which it is considered essential to the life of the country, the rules of distancing are put in place:

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The employer is responsible for the health and safety of employees in accordance with the French Labour Code and the texts governing the civil service (particularly Article L. 4121-1 of the French Labour Code). In this respect, the employer must implement actions to prevent occupational risks, information and training actions, and finally set up an appropriate organization and means.

In this context, the employer may:

- Raise awareness and invite its employees to provide individual feedback of information concerning them in relation to possible exposure, to the employer or the competent health authorities;
- Facilitate their transmission by setting up, if necessary, dedicated channels;
- Promote remote working methods and encourage the use of occupational medicine.

In the event of a report, an employer may record:

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

It will thus be able to communicate to the health authorities, on request, the information relating to the nature of the exposure necessary for any health or medical care of the exposed person.

For his part, each employee must implement all means to preserve the health and safety of others and himself (article L.4122-1 of the French Labour Code): employee must inform his employer in the event of suspected contact with the virus.

[…]

What to do if an employee shows symptoms of Coronavirus infection?

As mentioned above, employers have a general legal safety obligation with respect to their employees. If the employee shows serious symptoms, the employer must call 15 (health urgency services). If an employee is infected with coronavirus, the employer must immediately inform the employee to stay at home. The employer must also immediately clean the employee's workplace.

The employee must provide a work stoppage from his general practitioner. He will then be able to obtain financial compensation from the Health Insurance. If a collective agreement provides for the employee's salary to be maintained in the event of illness, this agreement will continue to be applied for the employee suffering from coronavirus.

The employer will also have to inform employees who have been in close contact with the employee affected by the virus and, if necessary, to place them in quarantine in order to prevent the virus from spreading throughout the company.

In this situation

n, the employer may, if its activity permits, put the employees to teleworking.

Conversely, if the activity requires a presence in the company, the employer may then apply for a part-time activity to compensate for the absence of these employees.

If the company's activity is judged indispensable, measures recommended by the INRS should be applied.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Purpose of processing: As regards the purposes of the processing operations, it should be noted that data processing operations in the context of employment relations may be subject to specific national provisions. Such derogations are expressly provided for in Article 88 of the GDPR. In France, the purpose of processing is to ensure the safety of the employees and/or their vital interests. The European Data Protection Supervisor confirms that:

- employers may collect health data relating to their employees or visitors provided that the principle of proportionality and data minimisation is respected, and insofar as national provisions allow;
- employers may request health check-ups only insofar as they are legally obliged to do so;
- employers may disclose the names of their infected employees only if national law so permits and after informing employees in advance. The dignity and integrity of individuals must be protected;
- employers may only obtain COVID-19-related data to fulfil their obligations and organize their work within the framework of national legislation.

Legal basis: The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law. In the employment context, the processing of personal data may be necessary for compliance with a legal obligation (in France, the health and safety of employees referred into French Labour Code) to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.

[…]

FRANCE 2/2

[06/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[...]

- Organise the maintenance of the activity by limiting the number of people present simultaneously at the workplace or in the same premises (staggered **working hours, etc.).**
- **Avoid** meetings and gatherings of people in small spaces.
- Encourage individual offices by allocating the number of employees present.
- Encourage communication by email, telephone, audio or video conferencing.

It is recommended that procedures be established for visitor and customer access:

- Limit the number of visitors or customers and organise queues.
- Provide general hygiene instructions.
- Make hydro-alcoholic solutions available as far as possible at the entrance to the buildings receiving the public.
- Set up a safety distance, or even specific devices (intercom systems, screens, etc.) for positions that are particularly exposed to the public.
- In areas where this is to be maintained, organize company catering by extending the opening hours, leaving more than one meter between seats at the table and introducing alternatives to collective catering.
- Remove magazines and documents from waiting areas or common rooms.
- Limit access to conviviality areas and other collective break areas.
- Ensure that handwashing stations are supplied with soap and preferably single-use paper. If access to sanitary facilities is not possible (couriers, staff on occasional trips) provide staff with hydro-alcoholic solutions.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

[...]

If the health situation requires all actors to be particularly vigilant, the French Data Privacy Authority (CNIL) invites individuals and professionals to follow the recommendations of the health authorities and to only collect data on the health of individuals who have been requested by the competent authorities.

Finally, health data may be collected by the health authorities, who are qualified to take the measures appropriate to the situation. The evaluation and collection of information on coronavirus symptoms and information on the recent movements of certain persons is the responsibility of these public authorities.

What the employer cannot do:

While everyone must implement measures appropriate to the situation, such as restrictions on travel and meetings or compliance with hygiene measures, employers may not take measures that could infringe on the privacy of the individuals concerned, in particular by collecting health data that would go beyond the management of suspected exposure to the virus. Such data is/are indeed subject to special protection, both by the RGPD and by the provisions of the French Public Health Code.

For example, employers must refrain from collecting, in a systematic and generalized manner, or through individual inquiries and requests, information relating to the search for possible symptoms presented by an employee/agent and his/her relatives. It is therefore not possible to implement, for example:

- mandatory body temperature readings of each employee/agent/visitor to be sent daily to his or her superiors;
- or the collection of medical records or questionnaires from all employees/agents.

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

[...]

The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art.9.2.c), as recital 46 explicitly refers to the control of an epidemic.

Retention period: Regarding the retention period, no specific provision is provided in our local regulation. To date, we recommend to implement a retention period with reference to the end of the state of emergency.

Please note, on February 28, 2020, France's Ministries of Health and Labour published a series of questions and answers to assist companies and employees concerned about workplace issues due to COVID-19. These questions and answers were then regularly updated (last updated today, on April 4, 2020).
Similarly, on March 6, 2020, the French Data Privacy Authority (CNIL) provided its own recommendations with guidelines concerning the handling of the health crisis with regard to personal data privacy.

- Employers must refrain from collecting information on possible symptoms displayed by employees/visitors and their relatives, be it in a general way or through individual inquiries and requests.
- It is therefore not possible to collect the body temperature of employees or visitors in a systematic way at the entrance of the employer's premises.
- However, employers can raise employee awareness to encourage employees to report to their employers or to health authorities their possible exposure to the virus.
- Upon request by health authorities, employers may communicate information relating to the health of employees and the nature of the exposure to the virus.

GERMANY

[06/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

- **Employees:** In case of employees whose temperature is to be measured by the employer, sec. 26 para. 3 sent. 1 Federal Data Protection Act (BDSG) is decisive. Pursuant to said regulation, such measuring procedure is only permissible if it serves to fulfil obligations under labour law and if there are no interests of the employee that are worthy of protection. However, an elevated temperature is not a compelling indicator of a corona infection, so that sec. 26 para. 3 sent. 1 BDSG cannot be applied for this purpose. Instead, the questioning of employees for (corresponding) symptoms or in case of reasonable grounds for suspicion a fever measurement by a (company) physician can be considered.
- **Suppliers:** The measurement of temperature in the case of suppliers is not legitimated under Art. 9 para. 2 GDPR. However, the query of general data (whereabouts, travel, etc.) can be justified under Art. 6 para. 1 lit. f GDPR, as there is currently an increased legitimate interest on the part of those responsible. However, this legitimate interest must be demonstrated, for example by citing the protection of customers and employees against infection as a reason.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

Under data protection law (Section 26 para.1 BDSG/Art. 6 para. 1 lit. f GDPR/ Section 26 para. BDSG/Art. 9 para. 2 lit. b GDPR) collecting and processing of personal data (including health data) of employees is permissible in order to prevent or contain the spread of the virus among employees.

This includes information in the cases,

- in which an infection has been detected or contact has been made with a person who is proven to be infected or
- in which a stay in an area classified as a risk area by the Robert Koch Institute (RKI) took place during the relevant period.

The employer must inform his employees in case of a confirmed infection in order to identify and clarify possible contact persons as quickly as possible. However, the disclosure of personal data of persons who are demonstrably infected for the purpose of informing contact persons is only lawful if knowledge of the identity is necessary for preventive measures with regard to contact persons.

What to do if an employee shows symptoms of Coronavirus infection?

If there is a suspected case of the Coronavirus in the company, the employer must inform the rest of the workforce about this case in order to identify and clarify possible contact persons as quickly as possible. The fact that this is a processing of personal data should not prevent this obligation. Processing data is lawful under Art. 6 para. 1 lit. b, d and f GDPR. Besides, suspected cases are subject to mandatory reporting since 1 February 2020. However, according to Sec. 8 of the German Protection against Infection Act, the obligation to report is only mandatory for the physician or other medical personnel who make the diagnosis, but not for the employer. Therefore, the employer is generally not obliged to report a suspicious case in the company to the public health authority. The health authority is informed of the suspected case by the doctor who is making the report.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The employer's duty of care obliges him to ensure the health protection of his employees. This also includes the appropriate reaction to the epidemic or pandemic spread of a notifiable disease. However, these measures must be proportionate. The data must be treated confidentially in accordance with the above-mentioned provisions of the BDSG and GDPR. After the respective processing purpose has ceased to apply (regularly, i.e. at the end of the pandemic at the latest), the collected data must be deleted immediately.

GREECE

[18/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The Data Controller is able to request from data subjects to disclose their or their relatives' personal data or special categories of personal data that are absolutely necessary for the purposes of prevention and/or limitation of contagion of COVID-19 in the Company.

As a result, the Data Controller is able to collect the information via the submission of questionnaires by employees or visitors (e.g. if they had recently travelled abroad or if any relatives are likely to or have already been diagnosed COVID-19 positive).

Additionally, the Data Controller is able to measure the body temperature of people entering the premises of the Company, given that this is the considered as the only available and effective measure for the above-mentioned purposes.

The said measures are lawful under the following circumstances: first, that the principle of data minimisation and proportionality are fulfilled, second, all appropriate organizational and technical measures have been taken in order to safeguard security of data and third, that the processing is not systematic, constant and general in a way that leads to profiling.

The processing of personal data for purposes related to COVID is regulated under the GDPR and the Greek Law 4624/2019, according to the Guidelines, issued by the Hellenic Data Protection Authority on processing of personal data for purposes related to COVID-19, as well as Legislative Content Act issued on the 25th of February 2020 (art.1 par. 4).

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

According to the Greek employment legislation (arts. 42, 45 and 49 of Law 3850/2010), the employee has the obligation to declare to the employer any circumstances that may put at risk the health and safety at work. In this context, the employee whose COVID-19 test is positive shall disclose this fact to the employer. The collection and processing of such data on behalf of the Data Controller must be carried out in any case in such a way as to safeguard confidentiality, security and integrity of personal data.

Therefore, the employer is not allowed to disclose such information to third persons, since this processing may lead to stigmatization and consequently, transfer is considered unlawful.

What to do if an employee shows symptoms of Coronavirus infection?

As described in the previous answer, the employee is required to communicate to the employer all circumstances that may put at risk the health and safety at work. The symptoms of COVID-19 infection is definitely a condition that need to be disclosed to the Data Controller. As a result, the employer shall notify the National Organization for Public Health in order to proceed to all necessary actions.

The collection and processing of such data on behalf of the Data Controller must in any case be carried out in such a way as to safeguard confidentiality, security and integrity of personal data.

The transfer of this data by the employer to third persons is considered unlawful for the reasons described above.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing is the prevention and limitation of COVID-19 contagion.

The lawfulness of the processing of personal data may be established under the following legal bases of article 6 (1):

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The lawfulness of the processing special categories of personal data (health data) may by established under the following legal bases of article 9 (2):

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(e) processing relates to personal data which are manifestly made public by the data subject;

The employer shall destroy personal data upon the termination of this situation of emergency. However, the special categories of personal data (health data) that are included in the health folder of the employee that are retained by the occupational doctor must be retained according to the respective legislation.

HUNGARY

[21/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The employer shall develop a pandemic action plan that supports the company to have an appropriate crisis management plan that includes the procedures, preventive measures and safeguards introduced; the measures to be taken in case of an infection; the privacy impact assessment of the proposed measures recommendations for responsibilities; the decision-making powers; competencies; development of proper communication tools, etc. Within the framework of the action plan, the employer shall prepare a detailed notification for the employees about the most important aspects of COVID-19.

The employer must develop its internal policies in accordance with the risk assessment. It determines the extent to which the employer may interfere into privacy in order to properly manage the pandemic situation.

Especially examining the employee's private travels concerning the destination and the date of the travel, as well as recording data about any contact with a person from a high-risk country may be allowed only in case of a high exposure in line with employees' privacy notice. The employer shall also request the employees to notify the employer they may have been affected by the virus and go to their doctor.

The above measure must also comply with the principal of data minimisation and the appropriate legal basis must be determined in all cases.

The Hungarian Data Protection Authority finds it acceptable for example to issue questionnaires for the employees but these may not include questions in relation to health history and the employees may not be request to attach any healthcare related documents.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The employee shall notify the appointed person about this fact in line with the employer's applicable internal policy. The employer may conduct the necessary investigation only based on a necessity and proportionality test put behind, however the data of the infected employee may not be disclosed to other employees. The company shall also define the appropriate technical and organisational security measures to protect the data.

What to do if an employee shows symptoms of Coronavirus infection?

There shall be a confidential channel ensured to report the symptoms of Coronavirus, the notification obligation is prescribed by the Labor Code, however, the method of reporting and necessity measures put behind shall be ensured by the company from the perspective of technical and organisational measures; with proper organizational separation, ensuring that these data are minimised and supported by proper interest balancing test; as well legal base is defined and disclosed.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Legal basis are doubled and shall be defined based on article 6 (1) f) or e) and article 9 (2) b) or h) and (3) of the GDPR depending on the exact circumstances of the data processing .

IRELAND

[19/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Measures taken in response to Coronavirus involving the use of personal data, including health data, should be necessary and proportionate. The Data Protection Commission (DPC) has advised that Employers would be justified in asking employees and visitors to inform them if they have visited an affected area and/or are experiencing symptoms.

Implementation of more stringent requirements, such as a questionnaire, would have to have a strong justification based on necessity and proportionality and on an assessment of risk. This should take into consideration specific organisational factors such as the travel activities of staff attached to their duties, the presence of vulnerable persons in the workplace, and any directions or guidance of the public health authorities.

Further to the above, more specific and intrusive questions must be limited to the minimum necessary to achieve the purpose of implementing measures to prevent or contain the spread of COVID-19.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

Identification of an individual infected by COVID-19 should be avoided in the interests of maintaining the confidentiality of the employee's personal data. The DPC advise that, an employer would be justified in informing staff that there has been a case, or suspected case, of COVID-19 in the organisation and requesting them to work from home. This communication should not name the affected individual. Disclosure of this information may be required by the public health authorities in order to carry out their functions. Controllers should also ensure they document any decision-making process regarding measures implemented to manage COVID-19, which involve the processing of personal data.

What to do if an employee shows symptoms of Coronavirus infection?

The DPC advise that employers would be justified in requiring employees to inform them if they have a medical diagnosis of COVID-19 in order to allow necessary steps to be taken. However, it is important to keep in mind that the recording of any health information must be justified and factual and must be limited to what is necessary in order to allow an employer to implement health and safety measures.

Employers should follow the advice and directions of the public health authorities, which may require the disclosure of personal data in the public interest to protect against serious threats to public health.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

In circumstances where organisations are acting on the guidance or directions of public health authorities, or other relevant authorities, it is likely that Article 9(2)(i) GDPR and Section 53 of the Data Protection Act 2018 will permit the processing of personal data, including health data, once suitable safeguards are implemented.

Such safeguards may include limitation on access to the data, strict time limits for erasure, and other measures such as adequate staff training to protect the data protection rights of individuals.
Employers also have a legal obligation to protect their employees under the Safety, Health and Welfare at Work Act 2005 (as amended).

This obligation together with Article 9(2)(b) GDPR provides a legal basis to process personal data, including health data, where it is deemed necessary and proportionate to do so. Any data that is processed must be treated in a confidential manner.

It is also permissible to process personal data to protect the vital interests of an individual data subject or other persons where necessary. A person's health data may be processed in this regard where they are physically or legally incapable of giving their consent. This will typically apply only in emergency situations, where no other legal basis can be identified.

No specific direction has been provided by the DPC around retention periods, however employers should not continue to process such data once the legal basis for such processing has expired.

ITALY

[15/06/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The companies that will adopt the Protocol for the regulation of measures to fight and contain the spread of the COVID-19 in the workplace will be able to request information on the travels made and the state of health of anyone accessing the premises or local offices, as well as to measure the body temperature, with reference both to employees and, where entry is necessary, to suppliers (for example, in the case of personnel in charge of sanitation activities or technicians working on maintenance of systems).

These activities shall, in any case, be carried out in compliance with the principles of necessity of processing and data minimisation.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

In the case of an employee declared positive for the Coronavirus, the company shall carry out internal investigations and collect information aimed at identifying the persons who have come into close contact with the positive subject, in order to communicate such data to the Health Authority and allow that the necessary and appropriate quarantine measures are applied. Indeed, it is necessary to remind that the data shall not be disclosed or communicated to third parties who are not subjects operating in the Police Force, in the National Civil Protection Service and in public and private organizations operating within the National Health Service.

The collection and processing of such data must in any case be carried out in such a way as to guarantee the confidentiality and dignity of the employees involved.

The company shall also define the appropriate technical and organizational security measures to protect the data.

What to do if an employee shows symptoms of Coronavirus infection?

The employee with symptoms of Coronavirus infection is required to inform the company that shall notify the competent healthcare authorities - through the emergency numbers for COVID-19 provided by the Region or the Ministry of Health - and to isolate the employee and other persons involved so that they do not come into contact with other people, containing the risk of contagion.

The collection and processing of such data must in any case be carried out in such a way as to guarantee the confidentiality and dignity of the employee. The company shall also define the appropriate technical and organisational security measures to protect the data. In conclusion, it is necessary to remind that the data shall not be disclosed or communicated to third parties who are not subjects operating in the Police Force, in the National Civil Protection Service and in public and private organizations operating within the National Health Service.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing is identifiable in the prevention of COVID-19 contagion; the legal basis is identifiable in the implementation of the anti-contagion security protocols pursuant to Article 1, no. 7, letter d) of the DPCM of 11 March 2020; the retention period can be set – if applicable - with reference to the end of the state of emergency.

LATVIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

In order to protect business and most importantly health of the employees and visitors, the employer/data controller can obtain information from the employees and visitors whether they have been abroad for the past 14 days and/or have they been in contact with COVID-19 sufferers or contacts. The employer for prevention purposes also may measure the temperature of the employees to determine whether they can perform their job duties. However, the employer shall ensure appropriate protection of such data and must ensure that all principles stipulated in the GDPR are fulfilled (for instance purpose limitation and data minimisation principle).

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If the employer learns that one of its employees is infected with COVID-19, the employer must contact the Latvian Centre for Disease Prevention and Control.

Disclosing this information to a third party other than the responsible authority violates person's right to privacy and data protection.

The employer also must take various steps to protect further transmission of COVID-19 in the workplace. For instance, the employer must be aware when was the employee likely infected by the virus and what transmission risks has this created in the office; who the employee contacted in person (employees, clients, visitors); which areas of the workplace require sanitary cleaning.

The employer has the right to inform other employees if the employer learns that one of its employees is infected with COVID-19 without disclosing the employee's name (or other personally identifiable information) and to inform employees that they are required to comply with the safety and health measures of COVID-19 prescribed by the authorities.

The collection and processing of such data must, in any case, be carried out in such a way as to guarantee the confidentiality of the employee involved and the employer also must limit access to such kind of data to only those employees who need it for the performance of their duties.

The employer shall also define the appropriate technical and organisational security measures to protect the data.

What to do if an employee shows symptoms of Coronavirus infection?

In case an employee shows symptoms of Coronavirus infection, the employer shall inform only the responsible authorities according to their competences (in this case Latvian Centre for Disease Prevention and Control).

If there is a reasonable suspicion that the employee is suffering from a disease, which endangers or may endanger his or her or other person's safety or health, the employer shall be entitled to order the employee to undergo an immediate medical examination. Though if an employee experiences symptom of novel coronavirus COVID-19 but refuses to undergo an immediate medical examination, the employer may (depending on the actual circumstances) consider employee's suspension from work.

Furthermore, if the employer has information about the employee being infected with COVID-19, it is the employer's obligation not to allow that employee to carry out his or her job duties and send him or her home.

However, if despite the employer's order, the employee nevertheless arrives at work and does not want to leave it, the employer has the right to call the State Police.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of processing may differ and must be determined on a case-by-case basis (for instance when measuring the temperature of the employees the purpose of processing should the safety of the employees and visitors); legal basis could be a public interest in the area of public health or to protect vital interests (Article 6 and 9 of the GDPR) or to comply with another legal obligation; the retention period should be set by a case-by-case basis (for example, personal data collected when measuring the temperature of the employees cannot be stored, gathered, compiled or otherwise used).

LITHUANIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

There is no specific regulation related to this question. It is up to the Employer/Data Controller what kind of measures it will take regarding the people who need to enter the premises of the company. While taking into consideration legal regulations, the Employer/Data Controller can set up internal rules to determine the conditions and circumstances of how and when people can enter the company's premises.

However, it is worth mentioning that according to the Law on Occupational Safety and Health of Republic of Lithuania, the Employer is obliged to ensure safe working conditions for the employees. It means that Employer must take actions to ensure safety of every single employee when allowing other employees on company premises.

In order to do that, the State Data Protection of the Republic of Lithuania provided statement that the Employer/Data Controller can ask the following information:

- Whether the person was traveling to a 'country of risk',
- Whether the person was in contact with a person traveling to a 'country of risk' or suffering from COVID-19,
- Whether the person is at home due to quarantine (without giving a reason) and the quarantine period,
- Whether the person is ill (without specifying a specific disease or other reason).

Also, the State Data Protection Inspectorate of the Republic of Lithuania noted that Employer/Data Controller has a right to ask its employees or visitors whether they have symptoms of COVID-19 or whether they have been diagnosed with COVID-19.

Depending on the responses received, different measures can be identified for each person or group of persons.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If the employee is tested positive for COVID-19, with this person's consent this data may be transferred to a personal healthcare facility of his/her choice. If the data is requested by the competent public authorities for public health purposes, the Employer/Data Controller should provide the employee's personal data. Data must be provided in accordance with the authority's instructions, for example if the data is provided for statistical purposes (how many employees are sick or isolated in the company) then the information provided should be anonymized.

The Employer/Data Controller cannot provide health information to other employees or clients by disclosing the infected employee's identity. However, if the employee was identified of having COVID-19 or having symptoms of COVID-19, the Employer/Data Controller has the right to notify other employees in order for them to take actions like to undergo quarantine, to work remotely, check health, and so on.

What to do if an employee shows symptoms of Coronavirus infection?

Kindly note that the employer has the right to ask his employees whether they have symptoms of coronavirus or whether they are diagnosed with COVID-19. If tested positive, the employee is required to notify the competent healthcare authorities and the company. The employer must be aware of this information in order to apply additional safeguards in the workplace – to oblige other employees who have worked or who have been in contact with an infected person to undergo self-quarantine, to enable conditions for medical examinations, to work remotely, etc. Please note that Lithuanian laws states that employer is obliged to require an employee to work from home, if there is a threat to health of other employees. If the employee rejects the request to work from home, the employer shall be entitled to remove the employee from the office without payment of salary (it is applied if there is a possibility to work from home). Further, kindly note that employer is required to follow Lithuanian health authorities' recommendations on how to ensure safe workplace (i.e., provide facilities for personal hygiene, to ensure surface disinfection, etc.).

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Possible purposes:

- safety of other people;
- public health purposes.

Legal basis:

- GDPR Art. 6 ph. 1 (c), (d); Art. 9 ph. 2 (i).
- The legal regulation does not indicate the specific period of time for Employer/Data Controller to handle the data related to COVID-19. However, the data should not be stored than objectively required, i.e., since the data will only be needed to the Employer/Data Controller during the quarantine period it means that the data should not be stored much longer after the end of the quarantine.

LUXEMBOURG

[01/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Under Luxembourg law, the Labour Code provides for an obligation for the employer to take all necessary measures to ensure the employee's health and safety at workplace. These measures may take the forms of prevention plans as well as imposing additional obligations on employees or suppliers entering the premises. Employers can oblige people to wear masks, gloves or to use hand sanitizer.

It is however not recommended to an employer to measure his/her employees' or suppliers' body temperature as such action shall be considered as a processing of personal data (the individual health status being a personal data) that shall be at all times governed by the principles of proportionality and data minimization.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

According to the statement issued by the Luxembourg Data Protection Authority (CNPD) in the context of the Covid-19 pandemic, employers are entitled to process infected employees' personal data in order to identify the potential date and place of infection and take the relevant measures.

Such information can be communicated to the national Health Authorities, competent to take necessary measures to prevent the pandemic to spread on the territory of Luxembourg. In the same statement, the CNPD has mentioned that the personal data collected by the employer shall not be communicated to other third parties or entities (other employees, service providers) without a clear justification.

In our understanding, it is clear that the employer is entitled to communicate with other employees who have been in direct contact of the infected employee on order to prevent the spread of the virus within the company.

However, the concerned employee shall be informed prior to such communication and his/her integrity and dignity shall be respected at all times.

What to do if an employee shows symptoms of Coronavirus infection?

The Luxembourg Labour Code provides for an obligation for the employee to take all necessary measures in order to protect his/her health and safety as well as the others'. In that sense, the employee who shows symptoms or has been in direct contact with an infected person shall inform the employer of such potential infection without undue delay.

The employer shall abide by the guidelines issued by the national health organizations and ask the employee to remain home isolated. As mentioned above, the employer is entitled to process such personal data and communicate them to the national Health Authority and the other employees who might have been in direct contact with such potentially infected employee. However, such disclosure must respect at all times the integrity and dignity of the individual.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

In our understanding and based on the statements released by the CNPD and the EDPB, the purpose of such processing of personal data is the prevention of the spread of the Covid-19 pandemic. There is no explicit legal basis on which the processing of personal data may be based.

However, the CNPD has released statements mentioning the right of employers to process such data. There is no explicit retention period of such personal data. However, the Law of 24 March 2020 mentions that the State of Emergency related to the Covid-19 pandemic will last for at least 3 months. In our understanding, the personal data may be retained as long as specific measures related to the pandemic may be taken by employers.

MALTA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

It is our understanding that, prior to admitting any persons into the workplace, an employer should be permitted to collect the relevant personal data, possibly including body temperature measurements, recent travel history, and recent contact with persons who are subject to self-isolation precautions.

This notwithstanding, the collection of personal data should be limited to only that information which is strictly necessary for the proper assurance of a safe workplace, and the processing of the obtained data should not include any processing which is not strictly related thereto.

Access to the data should be limited to a minimal number of persons, on a need-to-know basis only.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

It is our understanding that, in the case that an employee, who has been present at the workplace has tested positive for COVID-19, the employer may immediately initiate an investigation to determine the persons – both employees and third parties recently present at the work premises – with whom the infected employee has had contact.

Communications should ideally be issued in a manner which allows for immediate confirmation by the recipient. This means that an email can possibly be viewed as non-sufficient, and a more effective means of communication would be instant messaging (through approved channels) or possibly telephonic communication.

What to do if an employee shows symptoms of Coronavirus infection?

Any employees who have had contact, or shared a physical workspace, with the infected employee should be immediately informed that one of their colleagues has contracted COVID-19, and the necessary precautions, including quarantine leave and/or self-isolation, should be implemented immediately. It is understood that employees do not need to be informed of the identity of the infected employee, unless this knowledge is absolutely critical for reasons which the data controller becomes aware of.

Similarly, it is understood that third parties who have been present at the workplace, or who have had direct contact with the infected employee, should also be informed that an infection has occurred. Likewise, such third parties would not need to know the identity of the infected employee unless absolutely necessary.

As applicable or necessary, the appropriate health authorities should also be informed of the circumstances through the appropriate channels.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

It is our understanding that most data collection may be validly based on the employer's intention and obligation to protect the vital interests of the data subject or persons, in terms of Article 6(d) GDPR.
However, any data collection which specifically relates to information about the health of the given individual, is treated by the GDPR as a special category of personal data, and as such processing should be based on Article 9(2)(b) GDPR.
Furthermore, we consider that the retention period of the data in question should not exceed the appropriate amount of time necessary to ensure that the purpose of the data collection – i.e. ensuring the safety of the workplace – has been achieved.

NETHERLANDS 1/2

[07/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

1. Work from home instruction
When the employer is data controller it should instruct the employee to work from home as much as possible. The employer may refuse access to the office if this is necessary to provide a safe and healthy work environment for the workforce as a whole/others. For example if the general distancing rule of 1,5 meter distance cannot be guaranteed.

2. Monitoring health by employee/company doctor
For employees and/or suppliers that need to enter the office, the employer may only ask the employee/supplier to monitor their own health and measure their own temperature. If the employer suspects that the employee/supplier is ill, because he/she shows symptoms of a cold or the flue, the employer may refuse the employee/supplier access to the office and ask him/her to contact a doctor.

3. Thermal screening by employee/company doctor
Thermal screening of employees is only allowed if it is done by a (independent and registered) company doctor. The results thereof can only be shared with the individual employee concerned and, on an anonymous / aggregated level with the public health authorities. It is then up to the employee to decide whether or not they wish to share the results with the employer. If the company doctor concludes that the concerned employee is unfit for work, access to the work place can be refused to the concerned employee.

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

Following the strict interpretation of the law the employer is not allowed to ask whether the employee is tested positive for corona and process this information. If the employee is tested positive (by a doctor), the doctor will inform the municipal health service (“GGD”) and the GGD Protocol will take effect. The GGD Protocol consists of a contact inquiry, including (if applicable) cooperation with the employer on how to inform employees who have worked closely with the infected employee.

What to do if an employee shows symptoms of Coronavirus infection?

What measures are allowed to be taken?

Employees may be sent home if they show symptoms of the Coronavirus infection or when the employer is in doubt. The employer is allowed to request employees to monitor their own health.

What measures are not allowed to be taken?

Following the strict interpretation of the law the employer is not allowed to inquire on the nature of the disease, or process health data in any way.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

No legal ground for processing health data for prevention measures yet – “corona exception” to be defined by Dutch lawmaker.

*Please note that where this concerns health data, an exception following art. 9 GDPR is also necessary. As explained above, the Netherlands follows a very restricted approach to processing of health data by employers, and no specific lawful exception exists for this situation. On the other hand, the Dutch DPA acknowledged that in times like these, privacy should not stand in the way of providing healthcare and battling this pandemic. While this is not an official, lawful exception ex art. 9 GDPR, it could be argued that there is a (very narrow) window of opportunity for a “corona exception”. What the boundaries are of such exception and whether this also provides more room for employers to process health data is unclear. As soon as the Dutch DPA provides more guidelines on this topic, this paragraph will be updated.

If the Dutch legislator and/or Dutch Data Protection Authority were to introduce an exception to art. 9 GDPR, the following purpose and legal basis are most likely to be applied:
Purpose: the prevention of COVID-19 contagion.
Legal basis: most likely vital interest (art. 6 (1) (d) GDPR), following recital 46 GDPR.
Retention period: this could vary case-by-case depending on the specific reason for retention.

NETHERLANDS 2/2

[07/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[…]

What measures are not allowed to be taken?

The employer may not process health data in any way. This includes taking temperature or any other tests. On 24 April the Dutch Data Protection Authority (“Dutch DPA”) issued a press release about this matter. According to the Dutch DPA, organizations in non-compliance risk heavy fines. If organizations do not cease processing of health data of employees or visitors to check whether they have Corona, they are violating the GDPR and the Dutch DPA will use its enforcement powers.

Background
The Netherlands follows a very restricted approach regarding re-use and/or processing of health data. No specific lawful exception on article 9 (2) GDPR exists for this situation: exceptions (b) and (i) lack the required legal basis in national or union state law.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

POLAND 1/2

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

First of all, under special provisions adopted due to COVID-19 outbreak, the Chief Sanitary Inspector or the State Regional Sanitary Inspector acting under his authority may issue decisions imposing certain obligations on employers (and other legal entities or natural persons) as well as recommendations and guidelines on how to proceed in the execution of the tasks. Therefore, according to Polish data protection authority's opinion is that all actions to be taken by the Chief Sanitary Inspector and the designated entities will result from the provisions of law and the aforementioned decisions, guidelines and recommendations. These measures will constitute the legal basis for these activities, including the processing of personal data. Thus, if an employer performs certain preventive measures due to decision issued by Chief Sanitary Inspector or State Regional Sanitary Inspector, such decision will constitute a legal basis for processing personal data which is necessary for the execution of the decision.

When it comes to other measures that are not imposed by the decision (issued by relevant authority), there is no uniform approach in that matter.
It can be argued that some measures may be implemented under general rules set out in Polish labour code.

In particular, according to Article 207 of Polish labour code: The employer is responsible for health and safety in the work establishment.

In addition, Article 2092 provides that:
§ 1. If there is any possible danger to health or life, the employer must:

1) immediately inform employees about these dangers and undertake activities to ensure appropriate protection for them,

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If the employee test is positive, he/she is obliged to follow all instructions of relevant authorities. Non-compliance with such obligations is threatened by the different penalties imposed by Polish law. If in such a case the employee comes to work, the employer should notify the relevant authority and take all necessary actions so as to ensure that such employee does not put other employees at risk.

When it comes to communication addressed to the employees who have worked closely with the infected employee, the general GDPR requirements and labour law provisions (please see the answer to first question), in particular Article 2092, will apply. Therefore, employers should inform employees about COVID-19 cases and take protective measures but should not provide more information than necessary. In cases where it is necessary to disclose the name of an employee who is infected with the virus (e.g., in the context of prevention), the employees concerned should be informed in advance. Such information should be disclosed only to people whose security is in danger. The employer must however ensure that the dignity of persons concerned is protected as well as all relevant GDPR principles are complied with.

What to do if an employee shows symptoms of Coronavirus infection?

In order to limit the spread of coronavirus, the employer may instruct the employee to perform remote work for a fixed period of time (work specified in the employment contract, outside the place of permanent work) – regardless the fact of whether an employee shows symptoms of Coronavirus or not. When it comes to other preventive measures, the general rules indicated in the answer to question 1 will apply. Therefore, an employer can take actions if he/she is convinced that it is necessary to ensure the safety of employees as well as protection of their life and health. However, since there are no specific requirements in that matter, all preventive measure should be first thoroughly analyzed and justified so as to ensure that they are proportionate to the risk and non-discriminatory. In addition, all GDPR requirements will apply in that matter.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of processing personal data that may be indicated is the prevention of COVID-19 contagion as well as protection of employees' life and health. The legal basis for processing will differ depending on the actions taken as well as personal data processed (normal or sensitive data).

In the context of execution of the prevention measures, sensitive personal data may be processed on the basis of Article 9 paragraph 2 letter a), b), h) or i) of GDPR. When it comes to non-sensitive data, possible basis for processing are set out in Article 6 paragraph 1 letter a), c), d) or f) of GDPR.

When it comes to retention period – it should be specified in accordance with general GDPR rules and taking into account a specific purpose of processing.

POLAND 2/2

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[…]

2) immediately provide instructions to employees, in the event of a direct danger, enabling them to interrupt work and move away from the location of the danger to a safe place.

§ 2. In the event of a direct danger to health or life, the employer is obliged:

1) to stop work and issue instructions to employees to move away from the location of the danger to a safe place,
2) not to issue instructions to continue work until the danger has been eliminated.

Thus, as long as employer is able to demonstrate that specific preventive measures were taken due to the obligations indicated above, the processing of personal data necessary for proper fulfillment of such obligation will be justified. This may concern the request of information on the travels made and the state of health of people accessing the premises or local offices, as well as the measurement of the body temperature.

However, there is also an opposite approach, according to which activities indicated above require consent (in case of sensitive data – specific consent) of a data subject or – in case of non-sensitive personal data – legitimate interest could also be applied (provided that the balancing test allows for such processing).

Despite the legal basis for processing, general GDPR principles will apply – in particular the principle of data minimization, necessity, security and transparency.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

PORTUGAL

[01/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The Portuguese Data Control Authority (CNPD) has not published guidelines regarding personal data processing within the COVID-19 pandemic emergency. However, the Portuguese Health Authority (DGS) has published guidelines for the establishment of a contingency plan in companies. According to the Presidential decree that enacted the emergency state and the following Decree-Laws executing it, these guidelines must be duly followed.

In that regard, we have been advising our clients that they can collect personal data related to COVID-19 symptoms as part of the implementation of a contingency plan, in light of what other Control Authorities and the EDPB have advised. Any control measures should be adequate and proportional to the purpose they pretend to fulfill.

The applicable legal requirements may vary according to the type of data to be collected, and in some instances, the type of data subject (employees, employees' families, clients or services providers) can also have impact on the implementation of specific measures.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

According to the DGS guidelines, any infected employee should immediately report that situation to its immediate leadership.

Data controllers should only reveal health related personal data to the person responsible for the HR department and to the competent authorities. We have also advised to limit information collection to a specific and restricted group of people, whether it is the HR department, or a task force created for this purpose.

What to do if an employee shows symptoms of Coronavirus infection?

We have been advising our clients that if any employee shows symptoms of infection the company should warn other colleagues that might have be in direct contact with the said person, without revealing any information related to its situation or identification.

As a rule, infected employees are advised to only contact with the persons assigned as responsible for collecting such data, which normally is the person in charge of the HR department (as prescribed by safety and health rules in Labor context in Portugal).

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

We have been advising our clients to rely on one of the exceptions that GDPR foresees where health data is allowed to be processed, namely:

- Consent (not for employees as consent it not considered adequate)
- To comply with labor obligations and exercise labor-related rights
- To process the data for reasons of public interest in the area of public health

Regarding other data subjects (family members, customers, and service providers) the collection of such data can be based on consent.

For any other information that is not under a special category, companies may justify their processing under a legitimate interest, as we have no specific legal provision on this subject. A due balance test is needed, however, in order to verify if all the necessary technical and organizational measures are in place and to evaluate the adequacy and necessity, as well as the retention period, of the collected data.

ROMANIA

[19/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Romanian legislation (including the ones specifically adopted in relation to the Coronavirus prevention) does not provide specific measures that can be taken with respect to persons who need to enter the premises of the company. Similarly, the Romanian Data Protection Authority ("DPA") has not adopted any specific guidelines, recommendations or best practices in relation to the adoption of such measures but has mainly reiterated in a recent press release the necessity to observe the provisions of the GDPR with respect to processing of health-related personal data.

Therefore, in our view, the procedures adopted with respect to employees and/or suppliers entering the premises of the company will need to be carefully assessed from the perspective of the GDPR, considering the purpose pursuit by the company, specifics of the industry, number of employees and specifics of the working environment (i.e., whether there is closed contact between employees, etc.) and observance of data protection principles, in particular purpose limitation, data retention and data minimization.

With respect to employees, the measures will need to observe also applicable health and safety regulations, which may vary from industry to industry, as well as the instructions or recommendations issued by the healthcare professional within the company.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

In case of an employee whose test is positive for infection, the company will need to notify the competent relevant competent authorities (i.e., public health authorities). As regards communications addressed to employees who have worked closely with the infected employees, in line with applicable data protection regulations, disclosure shall be addressed only to a number of limited persons, such as the internal team or department dealing with the case or employees with which the infected employee worked closely (i.e., not the entire department or personnel of the company).

Similarly, communication addressed to other employees should not regard more information than necessary and adequate technical and organizational security measures to protect data should be, as well, implemented.

What to do if an employee shows symptoms of Coronavirus infection?

The regulations issued in Romania relation to COVID-19 do not set express obligations on private companies in case an employee shows symptoms, but it is reasonable to apply the same requirements as set out for public entities. Thus, the person showing the symptoms should be isolated and the case should be notified both on the 112 emergency number and to the local public health department. Until the arrival of the ambulance, it is prohibited to enter the isolation room except for the person designated for providing medical care to the suspect and who is wearing protective equipment and respects the medical precautionary procedures. Other requirements are provided in case the suspect is tested positive. However, in order to limit risks to employees, companies may consider applying preventive measures even until the health authorities inform of the result of the tests.

There are no specific provisions regarding the processing of personal data of employees showing COVID-19 symptoms and the general rules apply. However, considering the general obligation of the employer to provide all the information regarding the related labor health and security risks, we are of the view that disclosure of such information should be provided to a limited number of employees who are in contact with the respective employee (who shows symptoms of the infection).

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Romanian specific regulations, including the ones adopted in connection with the prevention of COVID-19 contagion do not address this aspect. Therefore, the general provisions of the GDPR with respect to choosing a legal ground and determining the retention period shall be applicable.

Also, with respect to the employer-employee relationship, the Romanian Special Telecommunications Service has provided a publicly available platform for the statements issued by data subjects and, respectively affidavits issued by the employer. Personal data collected through these documentations (which format is approved by the Internal Affairs Ministry) regard any trips or travels outside home permitted as an exception under current regulations. Legal basis is applicable in the Military Ordinance no. 3/2020 regarding the prevention measures with respect to COVID-19 contagion. Also, retention period can be set – if applicable − with reference to the end of the state of emergency.

SLOVAKIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The government has adopted various complex measures to combat the crisis, among which there are some that affect the employers and employees. Depending of the type of business, the Employer/Data Controller may measure the body temperature, with reference both to employees and, where entry is necessary, to suppliers.
Such possibility applies to hospitals and industrial factories (and is recommended to shops/grocery stores), i.e., it is not applicable generally to any company at this point.

The new rules have also introduced some exceptions to certain activities related to data processing and therefore to sanctions stipulated by GDPR and local regulation.

These activities shall, in any case, be carried out in compliance with the principles of necessity of processing and data minimization.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

One of the obligations of any employer is to ensure safety at workplace for all the employees. Such safety may be hindered by the Coronavirus. In the case of an employee declared positive for the Coronavirus, the company should take all the necessary measures to protect the employee and any of the employees that may have been in touch with such person, however the data should not be disclosed or communicated to unauthorized third parties.

The collection and processing of such data must in any case be carried out in such a way as to guarantee the confidentiality and dignity of the employees involved. The company shall also define the appropriate technical and organizational security measures to protect the data.

What to do if an employee shows symptoms of Coronavirus infection?

The employee with symptoms of Coronavirus infection is required to follow all the measures and recommendations adopted in legislation, therefore this responsibility rests primarily with the employee, not the employer.

Should the employer come into contact with such information and therefore to process such data, the collection and processing of such data must in any case be carried out in such a way as to guarantee the confidentiality and dignity of the employee.

The company shall also define the appropriate technical and organizational security measures to protect the data.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing is identifiable in the prevention of COVID-19 contagion and assurance of safety at workplace; the legal basis is identifiable in the implementation obligations stipulated by law (e.g., Act No. 124/2006 Coll., on Occupational Health and Safety; the retention period can be set – if applicable − with reference to the end of the state of emergency.

SLOVENIA

[02/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Employers are required to comply with the GDPR principle of data minimization and proportionality. Collect only such information as is necessary to ensure a safe working environment, depending on the organization of the work environment and prevent the spread of the virus.

Employers are required to take the necessary measures to ensure the safety and health of employees and other persons present in the work process but are obliged to comply with the principle of data minimization and collect only such information as necessary in order to ensure safe work environment and to prevent the spread of the virus. It is reasonable for the employer to require the employee to notify him on information required to ensure safety and health, e.g., if he has symptoms of Covid-19 virus or if his diagnosis has been confirmed or if he visited a particular critical country. In doing so, it is essential to ensure that workers are provided with transparent information regarding the collection of data, including the purpose of the processing and the retention period. The company shall also adopt appropriate security measures and confidentiality policies to ensure that personal data are not disclosed to unauthorized persons (accessible only to certain persons and not for example the whole department).

Employers/Data Controllers do not have a general authorization or requirement to measure the body temperature of employees/visitors. However, should the employer (considering special circumstances and the responsibility to ensure safety and health of employees) identify the measurement of the body temperature of employees/visitors as reasonable and necessary to minimize the potential of contagion at the work place, such measurement can be applied. In such case, however, the consent of the person to obtain this data should be given. Should the respective person refuse the measurement, the employer/data controller could deny entry to the premises of the company, in order to prevent contagion.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

If an employee tests positive for Coronavirus infection, it is in general the obligation of the employee to notify primarily the responsible authority of the persons (including his co-workers) who have been in contact with. However, considering the responsibility of the employer to ensure the safety and health of employees and other persons present in the work process, in case the employer is notified on the fact that the employee has tested positive, the employer shall as well collect information to identify persons who have been in contact with the employee and notify respective persons, but in principle on an anonymous basis, i.e., unless necessary, should not disclose the name of the infected person (in accordance with the principle of confidentiality and the principle of data minimization) as this could lead to discrimination and stigmatization.

The collection and processing of data must be carried out in such a way as to guarantee the confidentiality and dignity of the employee involved.

What to do if an employee shows symptoms of Coronavirus infection?

If an employee shows symptoms of Coronavirus, he should notify the employer, who shall then ensure safe work conditions, e.g., isolate the employee other persons involved so that they do not come into contact with other people, containing the risk of contagion.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The purpose of the processing is the prevention of COVID-19 contagion and the possibility of employees to benefit from intervention measures provided by new intervention regulations.

According to the Statement on the processing on personal data in the context of the COVID-19 outbreak (EDPR, 19 March 2020) “Employers should inform staff about COVID-19 cases and take protective measures but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g., in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.”

The legal basis in Slovenian national law for such collection of data can be identified in Article 5 (ensuring the safety and health of employees at work) of Health and Safety at Work Act, Article 45 (safe work conditions) of Employment Relationships Act and GDPR (Article 9) itself. The company should retain such data according to the purpose of processing for the period of state of emergency.

SPAIN 1/2

[01/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The Companies, acting in their capacity as data controllers, may request information about the trips made and the state of health of the persons accessing the workplace. Of course, these measures must be within the scope of the limits and guarantees established by the competent authorities and, in particular, the health authorities with regard to the safeguard of public health.

Therefore, the request for information to employees and external visitors on symptoms or risk factors would be fully justified under the provisions of the applicable regulations on data protection and prevention of occupational risks. Such a request for information would not require the consent of the data subjects, even if it concerns special categories of data (health data).

The SDPA even enables the security personnel to take the temperature of workers and suppliers at the time of access to the facilities, provided that it can be guaranteed that the data obtained from the temperature measurements strictly comply with the specific purpose of containing the spread of the virus, and not with other additional purposes, and that the data is not kept longer than necessary for the proper fulfilment of this purpose.

Similarly, the Employer may send health questionnaires to those persons who may have access to its offices. These health questionnaires may not be excessively detailed and should collect questions exclusively related to the disease (e.g., visits to countries with high prevalence of the virus in the incubation period of the disease, or existence of symptoms).
Of course, it is not necessary to emphasize that these data processing activities, and any others carried out by the Employer, must comply with the principles of proportionality and data minimization set out in the applicable regulations.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The Company will be able to find out whether the working person is infected or not, in order to design through its prevention service, the contingency plans that are necessary, or have been provided by the health authorities. This is justified by the application of the provisions set forth on the health and labour applicable regulations, in addition to the specific data protection. The Employer may, in accordance with such regulations and with the guarantees they provide, process personnel data necessary to ensure their health and take all the necessary measures dictated by the competent authorities, which also includes ensuring the health protection right of other personnel and avoiding the transmission within the company that can spread the disease to the population as a whole.
The personal data of any infected employee must be processed in accordance with the principles and guarantees set out in the applicable data protection regulations, and in particular guaranteeing the security, integrity and confidentiality of the information processed, and limiting the processing to the strict pursuit of the above mentioned purpose.

Therefore (as the SDPA has pointed out) the Companies will be able to know if the worker is infected or not, in order to design through their prevention service, the necessary contingency plans, or those that have been foreseen by the health authorities. In addition to the Occupational Risk Prevention Service and based on the legal criteria indicated, for operational needs this data may be processed by the areas involved in business continuity and crisis management. The above could be carried out in order to take those organizational measures necessary to maintain the activity of the Company and to avoid new infections, and in particular in relation to those employees who, due to their special functions and responsibilities may have been assigned to access to certain company facilities.

[…]

What to do if an employee shows symptoms of Coronavirus infection?

In accordance with the recommendations published by the SDPA, those employees who, after having had contact with a case of coronavirus, may be affected by this disease and who by applying the protocols established by the competent Health Authorities are subjected to the corresponding preventive isolation to avoid the risks of contagion derived from this situation until the corresponding diagnosis is available, must report this through the usual channels established by the Company.
Indeed, in accordance with Occupational risk prevention regulations and, particularly, regarding employees obligations in this matter (article 29 of the Spanish Occupational Risk Prevention Law) employees have the duty to cooperate with the employer to ensure safe working conditions which do not entail any risk for the health and safety of employees' and to contribute to the fulfillment of the obligations established by competent authorities in order to protect employees' health and safety at work.

Indeed, among other obligations, the employee shall even inform of any situation which may put at risk the security and health of employees at the workplace.

On this basis, employees' non-compliance with Occupational risk prevention matters are legally considered as a labour infringement which could ultimately be sanctioned by the employer in accordance with the types and classification of offences under the Workers' Statute and the applicable Collective Bargaining Agreement to the company.

Although under normal circumstances the employee on sick leave would be not obliged to inform the company of the reason for the leave, given the current public health crisis, this individual right may be waived in the face of the defense of other rights such as the safeguard of the health protection right of a group of workers in situations of pandemic and, more generally, the defense of public health of the entire population.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Depending on the particular circumstances associated with each processing of personal data, as well as the legal nature or the activity carried out by the Company as a data controller, they may collect and process this personal information in accordance with the following legal basis:

- Compliance with legal obligations: Article 14 of the Spanish Law on the Prevention of Occupational Risks states that workers have the right to effective protection in terms of health and safety at work. This implies a correlative duty for Spanish companies to protect the health of their workers and ensure their safety. In addition, the provisions by which the Spanish State has declared a state of alarm and has adopted the appropriate measures for the management of the pandemic, must be taken into consideration. Therefore, based on Article 6.1.c) and 9.2.b) of the European General Data Protection Regulation ("GDPR"), as well as the provisions of the SDPA, the processing of employee data, including those relating to their health, is permitted precisely to ensure the health and safety of patients, employees and collaborators (especially those who need to visit the Company's offices).

- Protection of the vital interest of employees: As established by article 6.1.d) and 9.2.c) of the GDPR, the processing of employee data is permitted, including those relating to their health, in order to protect the vital interest of the employee himself or of third parties − such as other employees or even patients or suppliers who may need to come to the Company's offices.

[…]

SPAIN 2/2

[01/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

[…]

This information can also be obtained by questioning the staff. However, the questions should be limited exclusively to find out about the existence of symptoms, or whether the working person has been diagnosed as infected or are subject to quarantine.

In regard to the information to be provided to the company's personnel who may have been in close contact with the infected employee/s, the relevant information will be provided in accordance with the principles of purpose and proportionality set out in the applicable regulations. This necessarily implies that, as far as possible, this information should be provided without identifying the person concerned in order to maintain his/her privacy. However, it is envisaged that this identifying information could be transmitted upon request by the competent authorities, in particular health authorities.

Similarly, in the event that the objective of ensuring the health of other employees and society cannot be achieved with partial information, or the practice is discouraged by the competent authorities, in particular health authorities, identifying information could be provided to those employees who have had close contact with the infected person.

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

[…]

The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller: In addition to the above, and in accordance with article 6.1.e) and 9.2, sections g and h of the GDPR, the processing of employee health data is also justified for the purpose of preventing the spread of the virus and to carry out the measures established by the health authorities.

Finally, regarding the retention periods to be observed by the Company health data, it is necessary to comply with the principles of data minimization and accuracy, i.e., to ensure, as far as possible, that the data are limited to what is necessary in relation to the purposes for which they are processed, accurate and, if necessary, updated. In accordance with the SDPA's pronouncement, the principle of minimization should also be applied with regard to the time limits for the storage of personal data. Furthermore, taking into consideration that personal health information collected from employees is mutable over time, nothing justifies its retention beyond the period during which the Employer must conduct relevant research to mitigate the effects of the spread of the virus within its company. With regard to other obligations, such as the blocking of personal data, the content of the purposes reported in each case will be taken into account to define the periods of blocking in each case.

SWEDEN

[01/04/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

Testing people who enter the premises is viewed as a significant integrity infringement, which measures can be taken is a labor law issue and the possible examination types which are dependent on the nature of the operations carried out at the workplace.

For measures such as tests of employees entering the premises, the big difference is weather such tests are voluntary or not. Voluntary tests can be carried out easily, however if there is a collective agreement at place, the union must be notified prior to the initiation of tests. If the tests are involuntary, these will be harder to carry out, and an analysis of the importance of the tests versus the integrity infringement must be carried out. The type of business can have a great impact on this analysis (more likely to be granted at a health care provider).

Other measures that can be taken at the workplace are setting up new guidelines for interactions at the workplace, such as lunch routines or meeting routines. These guidelines can be set up with short notice.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

The Swedish data protection authority, Datainspektionen, has explained that the employer is responsible for taking measures to ensure that employees are not exposed to any sickness or virus. Generally, it should be possible to inform the employees without naming the colleague that might have been affected by the virus. Naming the employee is only permitted in exceptional cases.

If the employer believes that it is necessary to name, the affected employee this employee must be informed beforehand. The employer must also take measures to protect the integrity of the employee and all information provided must be precise, correct and never infringe on the person affected.

As always, information sharing should be limited.

What to do if an employee shows symptoms of Coronavirus infection?

The starting point is that the employer is always responsible for the work environment and needs to ensure the safety of the employees. Having an employee showing symptoms of the virus could be dangerous for the workplace and it is therefore the employer's responsibility to manage and distribute the work to the best of all employees. In doing so, the employer may request an employee showing symptoms to stay at home. Either to work from home or, if this is not possible, stay at home with full salary. If sent home, the employee must always be able to come to the workplace with short notice.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

The legal basis for the Company to process personal data can be found in the labor law, where the employer has responsibilities towards the employees. However, the processing must be limited. The retention of any data cannot be longer than the fulfillment time of the purpose for which the data has been collected.

SWITZERLAND 1/3

[18/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

The Swiss law stipulates the employers' duty to protect the employees' health whilst at work. This includes providing the operational facilities and work processes to keep the risk of the COVID-19 infection as low as possible. The employers shall also comply with the hygiene and social distancing rules issued by the Federal Office of Public Health and the Ordinance on Measures to Combat the Coronavirus.

These measures must remain proportionate and to take the employees' personality rights into consideration:
• In the prevention plans employers can oblige employees or suppliers entering the premises to wear masks, gloves and to use hand sanitizer, and advise washing hands or avoiding handshakes;
• The number of persons present in a facility must be limited accordingly and gatherings of people must be prevented.
• In the case of company meetings, the organiser may require the participants to exercise their participation and voting rights exclusively in writing or online;
• In case of employees being or feeling sick or if anyone living in the same household exhibits symptoms, the employer can request them to stay home or work remotely in order to protect the other employees;
• Moreover, the employers must allow the employees at high risk to work from home or if the regular role does not allow for remote work, they have to provide them with an equivalent work.

The employers must undertake the necessary organisational and technical measures to enable this. If operational reasons require the full or partly presence of employees at high risk at the employer's premises, the employer has to meet the following requirements:
• All contact to other persons must be omitted, either by a separate office in a single room or separated work place with at least 2 metres distance.

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

An employee who has a medical diagnosis of COVID-19, is obliged to follow all instructions of the Federal Office of Public Health and to inform the employer of such an infection without undue delay.

The employer is entitled to process such personal data to keep the risk of infection as low as possible and this processing must be carried out in good faith and must be proportionate. In cases where it may be necessary to disclose the name of an employee, such information should be disclosed only to persons whose health is in danger – e.g. to employees who have been in direct contact with the confirmed employee, in order to prevent the spread of the virus. However, the concerned employee shall be informed prior to such communication and his/her integrity and dignity shall be respected at all times.

Wherever possible, within the organisation, any further identification of an individual infected should be avoided and the confidentiality of the employee's personal data shall be maintained - this wider communication should not name the affected individual. An employer would be justified in informing staff that there has been a case of COVID 19 in the organisation and requesting/recommending them to work from home.

Controllers should ensure they document any decision-making process regarding the processing of personal data implemented to manage COVID-19.

What to do if an employee shows symptoms of Coronavirus infection?

If possible, appropriate data on flu symptoms (e.g. fever) should be collected and passed on by those affected themselves and not by the employer. The affected persons themselves must report the incident.

The employee who shows symptoms or has been in direct contact with an infected person, shall be instructed not to come to the workplace, at least during the incubation period of the virus (i.e. usually up to 14 days) and, to the extent possible, allow for home office or remote work solutions. All preventive measure should be first carefully analysed and justified to ensure that they are proportionate to the risk and non-discriminatory.

The purposes of the collection and processing of this personal data shall be dedicated to enable protection of employees, partners, visitors, and the wider community from the threat of Covid-19. As explained in the previous question, the concerned employee shall be informed prior to such communication about him. Where possible within the organisation, any further extensive identification of an individual suspected for COVID-19 shall be avoided, controllers shall also document any decision-making process.

If an infection is medically confirmed, the employee will have to be quarantined (e.g., at home), and should not be allowed to return to the workplace until they are no longer contagious.

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

In the event of the Covid-19 pandemic, in circumstances where business organisations are acting on the guidance or directions of public health authorities, the purpose of processing of personal data by the employer is the prevention of the spread of this pandemic.

The legal basis for processing will differ depending on the actions taken as well as personal data processed (e.g. simple data or sensitive health data).

Article 328b of the Swiss Code of Obligation together with Article 4 of the Swiss Federal Act on Data Protection provide a legal basis to process personal data, including health data, when it is necessary and proportionate to protect health of employees. This processing must be carried out in compliance with the following principles:
• Health data is particularly worthy of protection and shall not be obtained against the will of the person concerned,
• The processing of health data shall be specific and proportionate with a view to preventing further contagions and is limited only to this what is necessary to achieving this goal,
• The collection and processing of health data shall be disclosed to those affected, so that the latter understand the meaning and purpose as well as the content and timing of the processing,
• Any data that is processed must be treated in a confidential manner (whenever possible).

If an EU resident's data is processed in Switzerland, the legitimate interest from the Article 6(1)(f) GDPR in collection and processing of personal data may be based on enabling protection of employees, partners, visitors, and the community from the threat of Covid-19.

[…]

SWITZERLAND 2/3

[18/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[…]

• Where close contact to other persons cannot be avoided, all appropriate protection measures need to be put in place (in particular personal protection gear as other technical/organisational measures).

Where neither remote work from home (regular or equivalent role) nor regular role with the above-listed safety precautions are possible, the employer has to provide an equivalent role at its premises in which he can ensure the above safeguards.

Before taking the prescribed measures, the employer must consult with the employees in question. In case none of these options is feasible or where the concerned employee does not agree with the measures, the employer is required to put the employee on paid leave.

Companies should only collect the necessary personal data - this means the minimum information needed to evaluate the risk that an individual carries the virus and take proportionate, risk-based measures. It is not recommended to measure employees' or suppliers' body temperature and note the individual health status.

The processing of this data shall be governed by the principles of proportionality and must be limited to the minimum necessary to achieve the purpose (more: https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1781027723).

As above-mentioned above, employer can from an employment law perspective instruct employees to stay away when they (or anyone else in their household) exhibit symptom or do not feel well.

[…]

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

[…]

It is with regards to the employer's duty of care, to protect employees and a wider public interest in managing a serious threat to health. Also, as employers have a legal obligation to protect their employees, this obligation together with Article 9(2)(b) GDPR provides a legal basis to process personal data, including health data, where it is deemed necessary and proportionate to do so.

No specific direction has been provided around retention periods; however, employers should not continue to process such data once the legal basis for such processing has expired / as long as employers may take specific measures related to the pandemic.

SWITZERLAND 3/3

[18/05/2020] **last updated**

What measures can be taken by the Employer/Data Controller with regard to people who need to enter the premises of the company (employers and/or suppliers)?

[…]

It is also advised to take this option from a privacy perspective, as it allows achieving the same objective without being as intrusive and prevents employees from answering extensive questions about the state of health posed by non-medical personnel, which may be unsuitable and disproportionate in this context. Also, when the use of digital methods for the collection and analysis of mobility and proximity data is considered, these must prove to be proportionate to the purpose of preventing infection.

In order to comply with the principle of transparency, the employees (and suppliers) may need to receive a privacy notice prior the collection of their data, describing what is the purpose, whether it will be shared with third parties (e.g., health authorities, etc.) and how long the collected personal data will be kept for this purpose.

The Federal Office of Public Health recommends also companies to implement a pandemic plan and the Influenza Pandemic Plan (2018) provides a basis and is available in German, French, Italian and English here: https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/pandemievorbereitung/pandemiehandbuch.html

It is important to add is that the Federal Epidemics Act (EpA, SR 818.101), which applies in the current extraordinary situation, fundamentally takes precedence over the Federal Act on Data Protection as a lex specialis and grants the Swiss authorities additional options to process personal data.

How to process data of the employee whose test is positive for infection and which kind of communications can be addressed to the employees who have worked closely with the infected employee?

What to do if an employee shows symptoms of Coronavirus infection?

For which purpose and on which legal basis the Company can process the collected personal data in the execution of the prevention measure? How long should the company eventually retain such data?

Contacts

Italy
Ida Palombella
Head of IP, Technology & Data Protection
ipalombella@deloitte.it

Austria
Sascha Jung
Partner
Sascha Jung s.jung@jankweiler.at

Belgium
Matthias Vierstraete
Senior Manager
mvierstraete@deloitte.com

Bulgaria
Reneta Petkova
Partner
rpetkova@deloittece.com

Croatia
Oreskovic, Jadranka
Senior Manager
joreskovic@kip-legal.hr

Cyprus
Gaston Hadjianastassiou
Partner
ghadjianastassiou@deloitte.com

Czechia
Jan Prochazka
Director
jprochazka@deloittece.com

Denmark
Helle Vestergaard Rasmussen
Partner
hrasmussen@deloitte.dk

Estonia
Julia Gramma
Senior Associate
jgramma@deloittece.com

Finland
Vesa Karvonen
Director
Vesa.Karvonen@deloitte.fi

France
Muriel Feraud-Courtin
Partner
mferaudcourtin@taj.fr

Germany
Heeke, Klaus
Partner
kheeke@deloitte.de

Greece
Ilias Koimtzoglou
Partner
ikoimtzoglou@kbvl.gr

Hungary
Peter Gondocz
Partner
pgondocz@deloittece.com

Ireland
Sean Smith
Partner
seansmith1@deloitte.ie

Contacts

Latvia
Samlaja, Ivita
Managing Associate
isamlaja@deloittece.com

Lithuania
Tomas Davidonis
Director
tdavidonis@deloittece.com

Luxembourg
Jean-Philippe Drescher
Partner
jpdrescher@dlaw.lu

Malta
Conrad Cassar Torregiani
Partner
ctorregiani@deloitte.com.mt

Netherlands
Marloes Dankert
Senior Manager
MDankert@deloitte.nl

Poland
Zbigniew Korba
Partner
zkorba@deloittece.com

Portugal
Joana Mota Agostinho
Senior Manager
jmagostinho@ctsu.pt

Romania
Georgiana Singurel
Partner
gsingurel@reff-associates.ro

Slovakia
Dagmar Yoder
Director
dyoder@deloittece.com

Slovenia
Andreja Skofic
Partner
askofic@deloittece.com

Spain
Dulce Maria Miranda
Partner
dmiranda@deloitte.es

Sweden
Johan Mikaelsson
Director
jmikaelsson@deloitte.se

Switzerland
Juerg Birri
Partner
jbirri@deloitte.ch

Deloitte.