How to manage data protection requirements in times of COVID-19

The COVID-19 outbreak implications for compliance with data protection laws

Employers might have to take measures to protect employees from becoming infected with coronavirus. Many employees are working from home, raising data protection considerations, especially regarding security and appropriate organisational measures. Some authorities expect that cyber security attacks and scams will increase during the COVID-19 pandemic because more employees are using unfamiliar hardware and software. (We've written separately about this.)

Additionally, some obligations in the EU General Data Protection Regulation (GDPR) and other data protection laws might now be more difficult to fulfil, for example because they are subject to deadlines.

Guidelines of data protection authorities

Many data protection authorities (DPAs) or equivalent (privacy) regulators have issued guidance on measures which are compliant (or not compliant) with the respective applicable data protection rules, for example:

Country / Region	Authority	Examples of important implications
Albania	Komisioner për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale	**Guidelines on processing personal data in accordance with the COVID-19 Hygiene and Sanitary Protocols** In compliance with the national obligation for employers to protect their employees' and other third parties' health according to the COVID-19 Hygiene and Sanitary Protocol, employers and business owners are required to collect personal and health information on COVID-19-related symptoms. However, they should not process more data than necessary for detecting COVID-19 symptoms and need to comply with information obligations. Employers informing staff about an infected colleague must take "utmost efforts to avoid naming individuals, and … should not provide more information than necessary." Identification would only be permissible in cases where circumstances make it inevitable. Read the original publication in Albanian and English here.
Australia	Office of the Australian Information Commissioner	**Guidelines on employers' privacy obligations to their staff** Employers can collect information from employees or visitors in relation to COVID-19

		but should only collect information which is reasonably necessary for preventing or managing COVID-19. Employers can, for instance, collect information on whether the individual (or a close contact) has been exposed to a known case of COVID-19 or whether they have recently travelled overseas and, if so, to which countries. Employers should only reveal names of employees or visitors potentially infected if necessary to prevent or manage COVID-19, and should disclose names only on a "need-to-know" basis to their staff. Read the original publication in English here.
Austria	Datenschutzbehörde	**Guidelines on data processing, FAQ and information on security measures for home offices** According to the Austrian DPA, it is permitted for risk prevention reasons to collect, process and store, for a short time, private mobile numbers of employees. However, employees cannot be forced to provide their private numbers. Regarding whether an infected employee can be disclosed by name to colleagues, the Austrian DPA states that this has to be evaluated carefully, and that general information might be sufficient and appropriate. The DPA also published some guidelines on security measures and warnings regarding malware. Read the original publications in German here.
Belgium	Gegevensbeschermingsautoriteit / Autorité de protection des données	**FAQs regarding possible measures taken by employers** Employers cannot make it compulsory to provide information, but can encourage employees to inform them when they have been in high-risk places. Read the original publication in Dutch and French here.

Canada	Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada	**Statement on applicability of data protection laws** The Commissioner states that, if data is processed on another legal basis than consent, data controllers need to be able to communicate to the affected persons the specific legislative authority under which this is done. Powers to collect, use and disclose personal information may be further extended only if a state of public emergency is declared. The statement also references several sets of guidance issued by different Canadian territories. Read the original publication in English / French here.
Denmark	Datatilsynet	**Short guidelines for employers** The Danish DPA states that recording and disclosing information that may be considered health information, e.g., that an employee is infected with new coronavirus, might be justified by the fact that it allows management and colleagues to take necessary precautions. Read the original publication in Danish here.
Dubai	Presidency of the Dubai International Financial Centre	**Presidential Directive No. (4) of 2020 in respect of COVID-19 Emergency Measures** This directive addresses privacy and cyber security considerations. In particular, it says employers should notify employees that they may carry out the general monitoring of IT systems and equipment to prevent misuse of employer assets during remote working. If they don't notify employees, employers must document "the clear purpose and benefits of any monitoring technologies". Employers should also notify employees that they may process employees' personal data for any reasonable purpose related to employees' health and safety as long as they do not process more information than reasonably necessary. Read the original publication in Arabic and English here.

Estonia	Andmekaitse Inspektsioon	**Guidelines on the processing of health data by employers** The Estonian DPA clarifies that special types of personal data, including health data, may not be processed on the basis of a "legitimate interest" but on basis of consent or if other legal justifications apply. The Authority suggests that employees voluntarily provide the employer with information about his or her health to the extent possible to safeguard their health and wellbeing and that of others and the society as a whole. Read the original publication in Estonian here.
European Union	European Data Protection Board	**Statement on the processing of personal data in the context of the COVID-19 outbreak** The statement advises that employers should inform their staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary; where it is necessary to reveal the name of an infected employee and the national law allows this, the concerned employees should be informed in advance and their dignity and integrity should be protected. With regard to the processing of telecom data, such as location data, the statement mentions that this is subject to national laws implementing the ePrivacy Directive. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals; and national legislative measures to safeguard public security are only possible if they constitute a necessary, appropriate and proportionate measure in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Read the original publication in English here.

Finland	Tietosuojavaltuutetun toimisto	**Guideline and FAQs regarding data processing** According to the Finish DPA, the information that an employee has returned from a risk zone and that an employee is in quarantine (without specifying the reason) is not health data. The guideline further states that, as a rule, an employer may not disclose an employee's name when informing third parties that the employee is diagnosed with COVID-19 or placed in quarantine. Read the FAQs in Finish, Swedish and English here.
France	Commission nationale de l'informatique et des libertés	**Guideline on possible measures by employers** Outlining that employers are responsible for employees' safety and security, the French DPA invites employers to regularly refer to the list of prevention measures at the workplace issued by the French Ministry of Labour to understand their obligations. Focusing on certain practices, the French DPA firstly explains that employers are prohibited from creating registers containing employees' temperature data, and from setting up automatic temperature checks systems, such as thermal cameras. Manual temperature checks with no data being stored do not fall under data protection law. Secondly, the French DPA stresses that only health workers may collect health data trough medical questionnaires or medical tests. Read the original publication in French here.
Germany	1. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) / Datenschutzkonferenz (DSK) *(the guidance was shared by some state DPA)*	**1. Guidance for employers** Collecting and processing personal data (including health data) from employees and visitors is permitted to prevent the spread of the virus, especially if: (i) an infection was detected or there was contact with an infected person; and (ii) an employee has stayed in a risk area.

		Disclosure of personal data – of people who have tested positive (or are suspected of being infected) – for the purpose of informing other people who may be at risk due to contact is only permitted in exceptional cases, i.e. if it is necessary for the contact person to know the identity of these persons to take precaution measures. Read the original publication in German here. See for example also the corresponding publications for Brandenburg here, for Lower Saxony here, for Mecklenburg-Hither Pomerania here, for North Rhine-Westphalia here, for Rhineland-Palatinate here, for Saxony-Anhalt here, and for Schleswig-Holstein here.
	2. Datenschutzkonferenz	**2. Resolution on data protection principles** The "Datenschutzkonferenz" stresses that processing of personal data must still be legally justified during the COVID-19 crisis. All planned measures should be carefully evaluated as to whether they are appropriate, proportional and effective; the "Datenschutzkonferenz" has concerns that measures to track individual infection patterns by using telecommunication data only are effective. Measures should be reversable and time-limited so as to apply only as long as necessary. Read the original publication in German here.
	3. Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg	**3. The Data Protection Authority for Baden-Wuerttemberg published additional FAQ for employers** Employers may temporarily collect and store employees' private mobile numbers for emergency contacts, but employees cannot be forced to provide their numbers. Read the original publication in German here.
	4. Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	**4. The Data Protection Authority for Rhineland-Palatinate published further guidelines regarding possible measures for employers**

		Obtaining detailed information on all employees from questionnaires is not necessary. Instead, employers should inform employees about areas with a higher risk of infection and request employees who have recently been in such regions inform their employer without needing to provide where exactly they have been and for how long. Read the original publication in German here.
	5. Bayerischer Landesbeauftragter für den Datenschutz / Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg	**5. The Data Protection Authorities for Bavaria and Brandenburg have published guidelines on technical and organisational requirements for home offices** The DPAs recommend measures to ensure confidentiality of information and to prevent storage of sensitive information on private devices. Read the original publication of the Bavarian DPA here and of the Brandenburg DPA here (both in German).
	6. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit	**6. Detailed guidance on data processing and security measures for electronic communication in the context of COVID-19** Employers may not question customers regarding symptoms because this is not effective. Employers may, however, ask employees whether they have had contact with infected persons or have travelled to a risk area in order to protect other employees from infections in the workplace. When informing employees about an infection of one of their colleagues, names should only be disclosed in exceptional cases; for example, it might be necessary to inform employees who have shared an office about the infection of a specific employee. The guidelines contain detailed information regarding evaluations of whether tools for electric communication meet the necessary safety standard and link further guidelines regarding safety for remote working. The Hamburg DPA mentions that deadlines for data subject rights continue to apply but that

		it may not sanction companies which fail to meet the deadlines due to COVID-19 in case the excess of deadlines was not very long and the company is small and does not have the necessary means to comply with the obligations in due time. Additionally, the DPA of Hamburg will currently not enforce fines. Read the original publication in German here.
Hong Kong	Privacy Commissioner for Personal Data	**Guidelines for employers and employees** It is generally justifiable for employers to collect temperature measurements or limited medical symptoms of COVID-19 information of employees and visitors solely for the purposes of protecting the health of those individuals but that all measures have to be necessary, appropriate and proportionate. Read the original publication in English and Chinese here.
Hungary	Nemzeti Adatvédelmi és Információszabadság Hatóság	**Guidelines on processing data related to the coronavirus epidemic** The Hungarian DPA especially stresses that "it must be examined in every case whether there are efficient solutions that pose less threat to the privacy of the data subjects". The DPA generally considers the requirements of screening tests with any diagnostic devices or the introduction of general mandatory temperature measurements disproportionate. Read the original publication in English here**.**
Iceland	Persónu Vernd	**Guideline and FAQ regarding measures of employers to prevent the spread of the virus** The Privacy Commissioner recommends using only yes-or-no questions to assess the risks: (i) Are you coming from a risk zone?; (ii) Do you experience symptoms?; (iii) Have you interacted with someone who recently came from a defined risk area? Read the original publication in Icelandic here. Read the additional FAQs in Icelandic here.
Ireland	Data Protection Commission	**General guidance regarding data processing with respect to Corona and FAQ**

		The Irish DPA stresses that the identity of an affected individual should not be disclosed to any third parties, including their colleagues, without a clear justification, and refers employers to the public health authorities to assess whether measures are appropriate ("Any questions about the appropriate measures that should be implemented to protect against COVID-19 should be addressed to the public health authorities."). Read the original publication in English here.
Israel	The Privacy Protection Authority	**Recommendations on privacy for individuals entering workplaces in the context of COVID-19** The Israeli DPA says that employers must check individuals entering the workplace in order to prevent the spread of COVID-19. However, employers must also make sure that they do not store the data they receive and any use of the data is in line with the privacy protection aspects of the Emergency Regulations.Read the original publication in Hebrew here.
Italy	Garante per la protezione dei dati personali	**Statement regarding permitted measures of employers:** The Italian DPA is of the opinion that the public health agencies have to deal with measures against COVID-19 and "employers must refrain from collecting, in advance and in a systematic and generalised manner, including through specific requests to the individual worker or unauthorised investigations, information on the presence of any signs of influenza in the worker and his or her closest contacts, or anyhow regarding areas outside the work environment." Read the original publication in Italian and English here. **FAQs on data processing in the context of COVID-19** The FAQs state that employers may detect the body temperature of employees or visitors at the entrance of the premises and offices prior

		to permitting entry. However, employers cannot record body temperature information as this is personal data. However, employers are permitted to record the fact that the temperature threshold set out in the law has been exceeded, and for documenting refusal of access to the workplace. Read the original publication in Italian and English here.
Latvia	Datu valsts inspekcijas	**Guideline on data protection in the context of COVID-19** The guideline stresses that data protection rights and obligations are still applicable. Regarding the rights of employers, it mentions, inter alia, that it might be permitted to obtain information from employees as to whether they have been abroad and in contact with COVID-19 in the last 14 days. Read the original publication in Latvian here.
Liechtenstein	Die Datenschutzstelle	**Guideline on data protection during the COVID-19 crisis** The guideline outlines that data protection rules continue to apply during a crisis such as the COVID-19 pandemic, but with some potential limitations. In this regard, employers may ask employees to work from home, may temporarily collect additional private contact information, and may ask about recent stays in risk areas, contacts with individuals infected with COVID-19 or the employees' health condition. Employees' responses may however only be collected on a voluntary basis. Read the original publication in German here.
Lithuania	Valstybinė duomenų apsaugos inspekcija	**Guideline on personal data protection and coronavirus COVID-19** The Lithuanian DPA states that it is "possible to process internal sets of personal data about employees" regarding whether an employee was traveling to a "country of risk", was in contact with a person traveling to a "country of risk" or is suffering from COVID-19, is at

		home due to quarantine (without giving a reason), or is ill (without specifying a specific disease or other reason). Read the original publication in English here.
Luxembourg	Commission nationale pour la protection des données	**Guideline on measures by employers** The Luxembourg DPA states that systematic and general collection of personal information is not allowed. Read the original publication in French and English here.
Mexico	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	**Guideline on COVID-19** With regard to data protection, the Mexican DPA provides information on the general obligation to comply with data principles, such as confidentiality, accuracy and transparency, as well as the need to implement strict technical and organisational measures. In addition, it clarifies the rights of employers, and outlines, in particular, that any communication made within the company about the potential presence of COVID-19 should not identify any employee individually. Read the original publication in Spanish here.
Netherlands	Autoriteit Persoonsgegevens	**Guidance for technical and organisational measures during home working** The Dutch DPA recommends taking care when using video chat services and paying extra attention to potential malware like phishing emails. Read the original publication in Dutch here. **FAQ for possible measures by employers** Only in the healthcare sector may employers check employees for infections during the corona crisis; all other employers are expected to follow the guideline of the Dutch Health Ministry (see here). Read the original publication in Dutch here.
New Zealand	Privacy Commissioner	**Guidance on COVID-19 and privacy FAQ**

		The FAQ answers what an employer should do if an employee is unsure whether they might have COVID-19 and chose to self-isolate; the New Zealand DPA does not recognise any health and safety imperative for the employer to disclose this information to other staff members. Rather, the employer should discuss with the employee in self-isolation how they want to deal with announcements to colleagues. Read the original publication in English here.
Norway	Datatilsynet	**Measures to prevent fraud and protect against malware during home office** The Norwegian DPA stresses the importance of being vigilant in times of crisis and links suggestions for secure working from home (see here). Read the original publication in Norwegian here.
Peru	Autoridad de Protección de Datos Personales	**Statement on collection of employees' health data in the context of health emergency** The Statement explains that employers may be permitted to collect personal data from employees, including health data, to guarantee safety and health at work, provided that such data collection is necessary and respects national (data protection) law. It is considered lawful for an employer to implement preventive measures aimed at detecting if any staff have contracted COVID-19, such as, for example, taking temperatures. Read the original publication in Spanish here.
Poland	Urzędu Ochrony Danych Osobowych	**Statement on temperature checks for the prevention of COVID-19** To prevent the spread of COVID-19, employers may process employees' and visitors' health data by measuring temperatures or implementing questionnaires on symptoms. Employers might even be required to conduct

		temperature checks if the Chief Sanitary Inspector considers it necessary. Read the original publication in Polish here.
Portugal	Comissão Nacional de Protecção de Dados	**Guidelines on the collection of health data of employees** The Portuguese DPA says that an employer may not collect and record employees' body temperature or other information related to health or possible risk-determining factors. Read the original publication in Portuguese here.
Russia	Roskomnadzor	**Statement on the processing of health data during COVID-19** The statement clarifies that although, as a rule, the processing of health data requires individuals' written consent, companies are not required to collect written consent to process their employees' and visitors' body temperature data obtained as a result of measurements taken to prevent the spread of COVID-19, provided that employees and visitors are notified of the measurements and have expressed their consent by implied conduct (i.e. agreed to the measurement). Read the original publication in Russian here.
Singapore	Personal Data Protection Commission	**Advisory on collection of personal data for contact tracing** Companies may collect, use and disclose personal data of visitors to premises for purposes of contact tracing and other response measures without consent during the crisis if this is necessary to respond to an emergency that threatens the life, health or safety of other individuals. Read the original publication in English here.
South Africa	Information regulator	**Guidance on processing personal information in relation to managing and containing COVID-19** South Arica introduced a guidance note regarding measures in connection with COVID-19 which stresses that "[r]esponsible parties

		must process the personal information of data subjects in a lawful and reasonable manner in order to detect, contain and prevent the spread of COVID-19" and setting out general rules for the lawfulness of processing and further obligations. The guidance note also contains some FAQs, it answers, inter alia, that employers are allowed to request specific information on the health status of an employee in the context of COVID-19 but information disclosed in this context should not be used to unfairly discriminate against such an employee. Read the original publication in English here.
Spain	Agencia Española de Protección de Datos	**Report on data processing activities related to reporting employees infected with COVID-19** According to the Spanish DPA, employees must inform their employer in the event of suspected contact with the virus, in order to safeguard, in addition to their own health, that of other workers in the workplace, and by doing so make it possible that appropriate measures can be taken; employers must process this data accordingly. According to the Spanish DPA, these activities are justified by the GDPR. Read the original publication in Spanish and English here. **Statement on temperature checks** Noting the intrusive nature of temperature checks, the Spanish DPA states that such personal data processing must meet the criteria defined by health authorities, and be used only if less intrusive measures cannot be implemented. Temperature checks must comply with applicable data protection law, ie the processing must have a legal basis (employers could rely on the obligation to guarantee employees' safety and health in the workplace); temperature checks should not be based on consent because affected persons cannot refuse to submit to checks without losing the possibility of entering premises so

		consent would not be voluntary. The Spanish DPA outlines several criteria for lawful temperature checks and necessary technical and organisational measures, and stresses that rights of data subjects must be guaranteed. Read the original publication in Spanish here.
Sweden	Datainspektionen	**FAQs regarding measures which be taken in the employment context** The Swedish DPA states that employers should avoid systematically gathering information about any illnesses from employees or their relatives and should refrain from taking measures which should be handled by authorities. Data protection requirements still apply and this means, among other things, employers may only collect necessary personal data which is necessary for the purpose in question and restrict access to such data within the organisation (on a 'need-to-know' basis). For instance, when informing employees about an infected colleague, employers should generally not use names and have to protect the integrity of the concerned employee. Read the original publication in Swedish here.
Switzerland	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter / Préposé fédéral à la protection des données et à la transparence	**Guidance on data processing by private persons** Health data is particularly protected and may not be obtained by private parties against the will of the persons concerned. All processing of health data by private parties must be purpose-related, proportionate and necessary (e.g. extensive questionnaires about the state of health by non-medical persons are considered inappropriate and disproportionate). Read the original publication in French, German, Italian and English here.
UK	Information Commissioner's Office (ICO)	**FAQ on data processing and COVID-19** ICO indicated that it will not penalise organisations that do not meet deadlines for

		answering data subject requests because they needed to prioritise other areas or adapt their usual approach. ICO also considers it reasonable to ask people whether they have visited a particular country or are experiencing COVID-19 symptoms before entering premises. Read the original publication in English here. **Additional guidance on workplace testing** ICO says that employers who want to test staff for symptoms of COVID-19 or the virus itself can do so by relying on the employment condition in Art.9(2)(b) GDPR, along with Schedule 1, part 1 of the Data Protection Act 2018. Prior to processing the data, employers should conduct a data protection impact assessment "focussing on the new areas of risk". Read the original publication in English here.
US	Health and Human Services (HHS)	**(A full update on HIPAA developments in the US can be found here.)** **OCR Bulletin on HIPAA Privacy and Coronavirus** In February, the OCR produced a bulletin reminding health industry participants about the existing legal avenues to share medical information to facilitate the fight against the COVID-19 threat. The guidance emphasised the ability to share information where necessary prevent or lessen a serious and imminent threat to the health and safety of a person or the public. The guidance also reminded readers that HIPAA does not typically apply to employers. Read the original bulletin here. **HHS Limited Waiver of HIPAA Sanctions** In mid-March, HHS announced that it would waive certain sanctions and penalties against hospitals that implemented a disaster protocol. A hospital that is within an emergency zone identified by the President's

		emergency declaration and that implements a disaster protocol will have a 72-hour grace period in which they will not be subject to sanctions or penalties for certain violations. Read the announcement here. **HHS Notification and Guidance Regarding Telehealth Services** Also in mid-March, HHS announced that it will exercise its discretion not to enforce HIPAA against medical providers who, due to the emergency and in good faith, adopt telehealth practices such as meeting with patients over video chat platforms. The notification can be found here; the guidance here.

"Adaptations" of GDPR rules which could be discussed with the competent DPA

The GDPR entails duties of controllers which might be more difficult to fulfil during the COVID-19 outbreak. For example:

- Art. 33 (1) GDPR requires that the controller notifies the competent DPA in the case of a personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it." The deadline is not an "absolute" deadline; if the notification is not made within 72 hours, it shall be accompanied by reasons for the delay. Therefore, controllers should make notifications as fast as possible and state – if relevant – how the COVID-19 crisis has affected the speediness of the notification process.
- Data subject requests generally have to be answered within a month's period (Art. 12 (3) GDPR); if a reply within a month is not possible, the data subject has to be informed. ICO already indicated that it will not penalize controllers in the UK where they need to prioritize other areas or adapt their usual approach during this extraordinary period, but also indicated that the general rules continue to apply. Controllers should in general take measures to inform data subjects if the deadline cannot be met. If this is not possible within the appropriate period, controllers can argue that they should not be penalised because of the COVID-19 outbreak.

Data protection issues relating to the use of technology to combat the pandemic

To fight the spread of COVID-19, governments around the globe are deploying and developing apps that help to fight the pandemic. For an overview of the different contact tracing apps worldwide, please see our series of blog posts, which will also look at whether companies should use contact tracing and, if so, what they need to do.