Hogan Lovells

Privacy 2040

Coronavirus and data protection – Guidance by data protection authorities

The table below sets out the guidance provided by data protection authorities in relation to the processing of personal data in the context of the fight against the coronavirus across various jurisdictions. The table is colour-coded by reference to the position expressed by each data protection authority. The most up-to-date version of this table is available here: https://www.hoganlovells.com/coronavirus-and-data-protection-guidance-by-DPAs.

Restrictive approach to data processing activities

Neutral approach to data processing activities

Permissive approach to data processing activities

Jurisdiction	Guidance	Key messages
Albania	Guidelines on the protection of personal data in the context of the measures taken against COVID-19 (in English)	The situation created by the spread of COVID-19 virus does not represent a lawful reason to disregard the right of each citizen to the protection of their personal data and therefore to disregard their private life, which combined, constitute a category of individual rights ensured by the Constitution but the Commissioner's Office recognizes the need for processing personal data. Besides the collection and the storage of personal data, it seems reasonable the need for increased transmission and exchange of such data among controllers and law enforcement institutions in the frame of the measures taken against COVID-19. Controllers may rely on legal bases set out in the Law on Personal data Protection to process sensitive and non-sensitive personal data to fight the COVID-19 pandemic. Purpose limitation, data deletion, and security and confidentiality principles must be applied to the personal data.

Jurisdiction	Guidance	Key messages
Austria	Guidance of the Austrian DPA FAQ on Coronavirus and Privacy Template for the collection of emergency contact information from employees Information on data security and home office (in German)	Employers can: • Process employees' personal data if they have tested positive, had contact with an infected person or stayed in a risk-area. • Process health data in order to fulfil their obligation to eliminate health risks in the workplace. • Collect and temporarily store personal contact details voluntarily provided by employees on the basis of legitimate interests. The Austrian DPA provides templates for this purpose. Any such personal data may only be processed for the purpose of COVID-19 containment and healthcare and must be deleted once storage is no longer necessary. Employers are not permitted to disclose the names of infected employees unless this is necessary to allow the employer to take effective precautionary measures. Employers may also transmit health data to the public health authorities given that the epidemic is considered a "disaster" under Austrian law. Employers must comply with data security requirements and should point out to their employees that hardware should be stored securely and that a secure Wi-Fi connection with a strong password (ideally also an encrypted VPN connection) should be used. There should be increased attention to phishing messages. The DPA provides more information here.
Belgium	Guidance on Covid-19 in the workplace Guidance on temperature measurement as part of the fight against COVID-19	Public health and disease prevention are not incompatible with the right to private life. Evaluation of health risks must be carried out by an occupational health doctor (not businesses or employers) who is competent to detect infections and inform the employer and those who have been in contact with the infected individuals. This processing of personal data can be based on Article 6(1)(c) and 9(2)(b) GDPR. The principles of proportionality, data minimisation and transparency must be observed. General and systematic testing, for example systematic temperature checking of workers and visitors, cannot be considered to be proportionate. Employers may not compel workers to complete medical questionnaires or questionnaires about their recent travel. In light of the principles of confidentiality and data minimisation, an employer may not reveal the names of the infected employee(s). The employer may only inform other employees of the situation without mentioning the identity of the data subject(s).

Jurisdiction	Guidance	Key messages
Council of Europe	Joint Statement on the right to data protection in the context of the COVID-19 pandemic (in English)	The right to data protection cannot be an obstacle to saving lives, but it is crucial that data protection principles are respected even in difficult situations. Legitimate bases for processing under Convention 108+ include data processing necessary for the vital interests of individuals and data processing carried out on the basis of grounds of public interest. The right to data protection does not prevent public health authorities sharing lists of health professionals (names and contact details) tasked with the distribution of FFP2 masks, epidemiological monitoring using anonymised data and the use of aggregate location data to identify unauthorised gatherings or movements of people away from severely-hit areas. Restrictions to personal data protections must be taken on a provisional basis during the emergency, for a strictly limited time and subject to safeguards. Communication to the public by health and government authorities should remain a priority, but publication of sensitive data of specific individuals should be avoided where possible. Employers may have to process more personal or sensitive data than normal and should respect the principles of necessity, proportionality and accountability. Employers should not process personal data beyond what is necessary to identify potentially exposed employees. If they are required by law to disclose certain data to state authorities for public health reasons, they should comply strictly with the underlying legal basis and return to "normal" when the state of emergency is over. Large-scale personal data processing by telecommunication companies, online platforms and internet service providers can only be performed when, on the basis of scientific evidence, the potential public health benefits override the benefits of alternative, less intrusive solutions.
Czech Republic	Processing personal data in connection with the spread of coronavirus (in Czech)	Sensitive personal data, including health data, may be processed on the basis of public health legislation (including legislation which is intended to address serious health threats). Regional hygiene stations and the Ministry of Health, Home Affairs and Defence are authorised to process personal data to the extent and for the purpose stipulated by the Act on public health protection. Appropriate measures include informing the population by sending SMS alerts. The legal basis of processing sensitive personal data where processing is necessary for reasons of public interest in the field of public health should be applied to this situation. Public or private entities should follow the guidelines and recommendations of the competent authorities.

Jurisdiction	Guidance	Key messages
Denmark	How about GDPR and coronavirus? (in Danish)	It may be justified for employers to register and pass on coronavirus information. An employer can to a large extent record and disclose information that is not so specific and specific that it can be considered health information when the situation necessitates that. The employer should consider: • Whether there is a good reason to record or disclose the information in question. • Whether it is necessary to specify the information, including whether the purpose can be achieved by "telling less". • Whether it is necessary to name names (e.g., the name of the person infected and/or in quarantine).
European Data Protection Board (EDPB)	Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak (in English) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (in English) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (in English)	Data protection rules do not hinder measures taken to fight the coronavirus, but controllers must ensure the protection of personal data. GDPR provides legal grounds for employers and public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject. For example this applies when personal data processing is necessary for employers for reasons of public interest in the area of public health or to protect vital interests, or to comply with another legal obligation. Additional rules apply when processing electronic communications data, such as mobile location data. Public authorities should aim to process location data anonymously, which could generate reports on the concentration of mobile devices at a certain location. When anonymous processing is not possible, Article 15 of the ePrivacy Directive enables member states to introduce legislative measures pursuing national security and public security. *For the purpose of scientific research* Personal data concerning health is a special category of data that may be processed for the purpose of scientific research, where applicable, to fight the COVID-19 heath crisis. However, personal data concerning health must still be processed pursuant to a separate legal basis for data processing (*e.g.,* consent, which *may* be freely given in this context). Member State law may also establish derogations that—together with a separate legal basis—would allow for processing health data. GDPR principles for processing must be observed in all cases, including where health data is transferred outside the EEA for the purpose of scientific research. *Use of location data and contact tracing tools*

Jurisdiction	Guidance	Key messages
		Applications of contact tracing tools should be part of a "comprehensive public health strategy to fight the pandemic" and their deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Location data may be transmitted to authorities or other third parties on an anonymised basis or with consent of the user. Preference should always be given to processing of anonymised data. Additional conditions apply to the re-use of location data. These are additional consent or as allowed by EU or Member State Law (e.g., national security, public security, or public interest). Contact tracing requires voluntary adoption by users, which does not necessarily mean that lawful processing is based on consent. Where storage/access to information is strictly necessary to provide the service explicitly requested by the user, the processing would not require consent. Careful consideration should be given to GDPR principles for processing personal data. In the context of contact tracing, this means: • The controller of any contact tracing application should be clearly defined and their roles and responsibility explained to users. • Purpose of the processing should be specific enough to exclude further processing for purposes unrelated to management of the COVID-19 health crisis. • Proximity data should be used rather than tracking location of individual users. • Appropriate measures should be put in place to prevent re-identification. • Only relevant information should be collected from the user's terminal equipment and only when necessary. A data protection impact assessment (DPIA) must be carried out before implementing contact tracing tools as the processing is considered likely high risk. The EDPB strongly recommends the publication of DPIAs.

Jurisdiction	Guidance	Key messages
European Data Protection Supervisor	Monitoring Spread of COVID-19 (in English)	Data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics. • Data anonymization: Effectively anonymised data fall outside of the scope of data protection rules. However, effective anonymization requires more than simply removing obvious identifiers such as phone numbers and IMEI numbers. Data aggregation can provide an additional safeguard. • Data security and data access: Where third parties are used to process information, these third parties have to apply equivalent security measures and be bound by strict confidentiality obligations and prohibitions on further use as well. It would be preferable to limit access to the data to authorised experts in spatial epidemiology, data protection, and data science. • Data retention: Data obtained from mobile operators should be deleted as soon as the current emergency comes to an end and any solution should be recognised as extraordinary (i.e., deployed because of the specific coronavirus crisis).
Estonia	Can an employee be required to tell everything about their health? (in Estonian)	The legal basis for processing of health data must not be legitimate interests. In some cases, employers are required by law to obtain a medical certificate before commencing work, but this applies only in certain areas such as food handling, healthcare and animal husbandry. It is unlikely that the government will be able to create a right for employers to process health records in emergency situations. The Health Board has currently restricted coronavirus testing to those with symptoms and those without who have paid. It is therefore crucial that employers and employees voluntarily provide their employer with health information that will allow the employer to organise work as safely as possible. The principle of data minimisation should be adhered to.

Jurisdiction	Guidance	Key messages
Finland	Data protection and limiting the spread of coronavirus (in English, also available in Swedish and Finnish)	Processing personal data to combat COVID-19 is permitted. Processing of personal data must be necessary and proportionate. Information that an employee has contracted coronavirus is health data, but information that employees have returned from a risk zone or are in quarantine are not health data without more. It is all personal data, however. The Finnish Act on the Protection of Privacy in Working Life and Contagious Diseases Act could both apply. If an employee is diagnosed with COVID-19, the employer may not name the employee in question. They can inform other employees of the infection or potential infection in general terms and instruct them to work from home.
France	Coronavirus (Covid-19): reminders from the CNIL on the collection of personal data (in French)	Employers must refrain from collecting in a systematic and generalised manner, or through individual inquiries and requests, information relating to possible symptoms presented by an employee / agent and their relatives. It is therefore not possible to implement, for example: • mandatory readings of the body temperatures of each employee / agent / visitor to be sent daily to their hierarchy. • or the collection of medical sheets or questionnaires from all employees / agents. The assessment and collection of information relating to symptoms of coronavirus and information on the recent movements of certain people is the responsibility of public health authorities.

Jurisdiction	Guidance	Key messages
Germany **(Conference of German DPAs; DPA of Baden-Wuerttemberg)**	Guidance of the Conference of German DPAs ("Datenschutzkonferenz") (in German) Guidance of the DPA of Baden-Wuerttemberg (in German)	Only the public health authorities, not the employer, have investigative and intervention powers. In case of doubt, employers are therefore requested to contact the health authorities and not to collect health data on their own initiative, and certainly not against the will of their employees. Employers may collect and process personal data (including health data) of employees and visitors in order to detect whether they were tested positive themselves, had contact with an infected person or stayed in a risk-area (legal bases: Sec. 26(3) FDPA and Art. 9(2)(b) GDPR regarding employees; Art. 6(1)(f) GDPR, Art. 9(2)(i) GDPR, Sec. 22(1) No 1(c) FDPA for visitors). The data may only be processed for a specific purpose (COVID-19 containment) and must be deleted after the end of the pandemic, at the latest. Employers are generally not permitted to disclose the name of infected employees, as this could lead to social stigmatization and discrimination. Exemptions may apply where disclosure of the name is necessary in order to allow the employer to take effective precautionary measures. Employees may be obliged under employment law to inform the employer in case they are infected with the virus. As a consequence, they may disclose information to their employer about persons they have been in contact with (legal basis: Art. 6(1)(f) GDPR).

Jurisdiction	Guidance	Key messages
Gibraltar	Data protection and coronavirus: what you need to know (in English)	Data protection will not, in principle, prevent organisations from sharing information quickly or adapting the way that work is conducted. Proportionality must be favoured when proposing actions. If something feels excessive from the public's point of view, it is probably disproportionate. • Keep staff informed about cases within the organisation, without providing more information than necessary. • While employers have an obligation to protect their employees' health, this does not necessarily entail gathering a lot of information about them. • It is reasonable to ask staff to inform the organisation if they have visited a particular country or are experiencing COVID-19 symptoms and data protection law will not stop the sharing of employees' health information with relevant authorities for public health purposes. In principle the Commissioner will not take regulatory action where financial or human resources are diverted away from usual compliance or information governance work during the pandemic if an organisation is seen to be acting reasonably and can justify their need to prioritise other areas or adapt their usual approach.
Global Privacy Assembly	Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic (in English)	Addressing the challenges of the coronavirus pandemic requires coordinated responses at national and global levels. Universal data protection principles will enable the use of data in the public interest and still provide the protections the public expects. This statement is intended to set out support for public bodies and health practitioners to be able to communicate directly with people, and scientific and government bodies to coordinate nationally and globally, to tackle the current COVID-19 pandemic.

Jurisdiction	Guidance	Key messages
Greece *(with thanks to NIKOLINAKOS & PARTNERS LLP)*	Guidelines for processing of personal data in the context of managing COVID-19 (in Greek)	Employers may legally process personal data for the purpose of protecting their health and that of their employees. Extra care must be taken to observe the principles of purpose limitation, proportionality and security of processing. Personal data protection legislation will not be applicable to verbal communication of data concerning health. Burdensome measures such as temperature measurement at the entrance to the workplace can only be carried out after any other available measure has been excluded. If disclosing information about deceased persons leads to indirect identification of the natural persons the deceased were connected to might mean that data about those deceased persons is subject to GDPR. Disclosure of data subjects' health condition to third parties is prohibited if it results in prejudice and stigmatisation.
Hungary	Information on processing data related to the coronavirus epidemic (in English)	If an employee reports possible exposure to their employer or the employer suspects exposure has happened due to data provided by the employee, the employer may record the data of the report and the personal data of the employee concerned. It acceptable to have the employees complete questionnaires, but questionnaires may not include data concerning the medical history of the data subject and the employer may not require employees to enclose health documentation. The legal basis for processing of personal data can be legitimate interests or performance of public tasks, and the legal basis for health data processing can be Article 9(2)(b). Requiring screening with any diagnostic device, in particular a thermometer, is disproportionate. In individual cases employers can call for individuals to be tested by health professionals on the basis of a risk assessment or report from an employee.

Jurisdiction	Guidance	Key messages
Iceland	COVID-19 and privacy (in Icelandic)	Measures taken to respond to COVID-19 involving the processing of personal information, including health information, must be necessary, proportionate, and based on information and guidance by relevant authorities. Information that a person is quarantined is generally not considered to be sensitive personal information, but it is important to have regard for the data minimisation and fairness principles. Health information should be considered to be sensitive personal information. For employers: • General information that one or more employees are currently quarantined does not fall under the Privacy Act, and such statistics may generally be disseminated. • Disclosing the name of an employee diagnosed with COVID-19 to others should be avoided, though it may be necessary to inform the health authorities of the employee's name. • Employers should only request information from their employees that is needed using yes/no questions. • Temperatures may be measured if the consent of the employee has been obtained.
Ireland	Data Protection and COVID-19 (in English)	Data protection law does not stand in the way of the provision of healthcare and the management of public health issues. Nevertheless there are important considerations which should be taken into account when handling personal data in these contexts, particularly health and other sensitive data, including: lawfulness, transparency, confidentiality, data minimisation and accountability.

Jurisdiction	Guidance	Key messages
Isle of Man	Coronavirus, Data Protection and Freedom of Information (in English)	Data Protection law does not stand in the way of the provision of healthcare and the management of public health issues. There are specific conditions in data protection law that makes healthcare processing—including disclosures—lawful, though the processing is still subject to appropriate safeguards. Employers and other organisations have a general obligation to protect the health of their staff and volunteers, so it is reasonable to ask if they have returned to the island recently and are required to self-isolate or if they or others close to them have experienced coronavirus symptoms. No more information should be asked for than is necessary and personal data must be accurate. There should be appropriate measures in place to ensure data is secure and that information is not kept longer than necessary. If a member of staff becomes ill with coronavirus, their colleagues should be told but that does not mean provide the name of the affected employee.
Italy	Joint protocol for regulating the measures in order to contrast and to reduce the spread of COVID-19 at the workplaces[1]	Companies are allowed to collect information about COVID-19 symptoms or location of their employees within the anti-contagion safety protocols aimed at combatting and reducing the spread of COVID-19 at the workplace. GDPR privacy principles (e.g., minimisation and retention) and the other relevant requirements (i.e., privacy notice, written instructions to persons in charge, and security measures) must be considered.
Jersey	Data Protection and Coronavirus (in English)	Public bodies and health practitioners are not prevented by privacy laws from sending public health messages or using appropriate technology to ensure expedient consultations and diagnoses. Public bodies may undertake a greater level of personal data collection and sharing to protect against serious threats to public health. Jersey law provides for an explicit basis for the processing of personal data where it is necessary for reasons of public interest in the area of public health. This includes protecting against cross-border threats to health and ensuring a high standard of quality and safety of healthcare and social care. Any processing must however be necessary and proportionate and carried out with the appropriate safeguards in place to protect the rights and freedoms of individuals in respect of their personal information. The current circumstances will be taken into account when assessing compliance with data protection law.

[1] This protocol, executed between the Government and main trade union associations on 14 March 2020, superseded initial guidance published by the Italian DPA on 2 March 2020.

Jurisdiction	Guidance	Key messages
Lithuania	Personal Data Protection and Coronavirus (in English)	Personal information about employees can be processed in accordance with the principle of data minimisation by including only information about whether the person was travelling to a country of risk, whether they were in contact with a person travelling to the country of risk, whether the person is at home due to quarantine and whether the person is ill. Employers may ask their employees if they have a diagnosis or symptoms of COVID-19. This does not imply that employers can document such information or compile relevant data files. Data protection principles must be observed when personal data is shared with public authorities for public health purposes. Requests for personal data must be assessed on a case-by-case basis. Employers should refrain from collecting temperature readings from staff or visitors, medical records or similar.
Luxembourg	Coronavirus (COVID-19): CNPD recommendations relating to the collection of personal data in the context of a health crisis (in French)	While private bodies may implement measures to contain the coronavirus (e.g. travel restrictions. hygiene measures), such measures must take into account the privacy of the data subjects. Organisations should therefore avoid systematic collection of data about coronavirus infection symptoms of employees, externals and relatives, particularly by means of daily body temperature measurements, medical questionnaires which have been prepared in advance, or requesting that visitors sign a pre-written declaration stating that they have no symptoms or that they have not recently been travelling to a risk area. The identity of data subjects (potentially) infected may not be disclosed to third parties or colleagues without clear reasons.
Malta	Processing of personal data in the context of COVID-19 (in English)	The appropriate legal basis for the processing of sensitive health data is that it is necessary for reasons of public interest in the area of public health. Controllers must comply strictly with instructions provided by public health authorities to prevent the spread of COVID-19, including any processing of personal data necessary to comply with national laws. Appropriate security measures must be taken. The Office of the Information and Data Protection Commissioner refers individuals to the EDPB's statement on data processing.

Jurisdiction	Guidance	Key messages
Netherlands	My sick employee (in Dutch)	Employers should not normally draw conclusions about the health of individual employees, for example by keeping track of where they have been or recording their temperature. However, employers can call in the occupational health and safety service or company doctor to check for corona.
Norway	Coronavirus and privacy (in Norwegian)	Employers can process specific categories of personal data when necessary to carry out employment law duties or rights. Information that someone is infected with the coronavirus is considered health information. Information that an employee has returned from a so-called "risk area" is not to be considered health information. Information that someone has been quarantined (without giving further details on the cause) is not to be considered health information.
Poland	Statement by the President of UODO on the coronavirus (in Polish)	The GDPR cannot be seen as an obstacle to the fight against coronavirus, The provisions of the special COVID-19 act (adopted on 2 March) give the General Sanitary Inspector the right to issue decisions imposing certain preventive obligations on employers, whereas the Prime Minister may impose certain obligations on all entrepreneurs, both of which correspond with the GDPR provisions (Article 9.2(i) and 6.1 (d)), According to Recital 46 GDPR the processing of personal data is lawful also when this is necessary to protect an interest which is essential for the life of the data subject, including monitoring of epidemics and their spread.
Romania	Processing of health status data (in Romanian)	Health data can be processed under Article 9(2)(a), (b), (h) or (i). The relevant information required under Articles 13 and 14 GDPR must be provided to affected data subjects in a concise, transparent, intelligible and easily accessible manner. This can be done using a website. The name and health condition of a particular person can only be disclosed in a public space with the prior consent of the affected person.

Jurisdiction	Guidance	Key messages
Russia	Guidance regarding use of thermal imagers and related processing of data on body temperature of employees and visitors (in Russian)	Information about body temperature is a special category of personal data, which can be processed without the consent of the data subject if carried out in accordance with labour legislation. Employers may request information about the health status of their employees. The consent of visitors to the organisation to thermal imaging is manifest in their actions of choosing to visit the organisation. Employees and visitors must be notified that temperatures are being measured. The information should be retained only for one day.
Slovakia	Coronavirus and processing of personal data (in Slovak)	The indication of the measured temperature falls within the processing of a specific category of personal data, and for the lawful processing of such data, the GDPR provides for special conditions in Article 9 and the disposal of the legal basis in Article 6.
Slovenia	Responsible behaviour is crucial during a viral crisis (in Slovenian)	Competent authorities have to make case-by-case assessments and determine what information is needed to protect people's vital interests.
Spain	Report on data processing in relation to COVID-19 (in Spanish; in English) FAQs on data processing in relation to COVID-19 (in Spanish; in English)	The Spanish DPA appears to favour Article 6.1(d) GDPR as the legal basis for processing (i.e. where the processing is necessary in order to protect the vital interests of the data subject or of another natural person). In accordance with labour and occupational risk laws, employers may process employees' data without relying on their consent, and ask them specific questions on their health status (extensive health questionnaires or ones with questions unrelated to COVID-19 are not permitted). Notice of an infected employee to the rest of the staff must be carried out on a no-name basis as a general rule. The Spanish DPA does not oppose temperature screening, but it must be carried out in accordance with labour and occupational risk laws, and by appropriate personnel. Following public authorities' directions would generally not entail a breach of GDPR rules. GDPR principles must still be complied with.

Jurisdiction	Guidance	Key messages
Sweden	Coronavirus and personal data (in Swedish)	Information that someone has contracted coronavirus is sensitive personal data, but information that someone has recently returned from a high-risk area is not. Information that someone is in quarantine (without more) is also not sensitive personal data. However, even if information about returning from risk areas or being in quarantine is not sensitive personal data, it can still be personal data. There must be a legal basis for processing and the fundamental data protection principles must be observed.
Switzerland	Legal data protection framework for coronavirus containment (in English, also available in German, French or Italian)	Private parties, including employers, must comply with the Federal Data Protection Act. Under this Act, health data are particularly worthy of protection and may not be obtained by private parties against the will of the data subject. Processing of health data must be proportionate and purpose-specific. Where possible, appropriate data on flu symptoms such as fever should be collected and passed on by those affected themselves. The collection and further processing of health data by private third parties must be disclosed to the data subjects so that they understand the purpose and scope of the processing as well as its content and time frame. Processing of medical data such as body temperature must be kept to the minimum necessary and the data must be deleted once the pandemic threat has ceased to exist at the latest. Answering extensive questions about the state of one's health to non-medical persons is inappropriate and disproportionate.
United Kingdom	Data protection and coronavirus: what you need to know (in English)	The Government, NHS and health professionals may send public health messages to individuals by phone, text or email, as these do not constitute direct marketing. The ICO will take the compelling public interest in the current health emergency into account regarding compliance. If data protection practices do not meet an organisation's normal standard or responses to information rights requests take longer, the ICO will not take regulatory action as they understand the need to prioritise other areas. The ICO will tell people that they may experience delays when making information rights requests during the pandemic. Employers should keep staff informed about cases but there is no need to name individuals and employers should not provide more information than is necessary. Data protection law is not an obstacle if it is necessary to share information with public health authorities.