

Covid-19 update DATA PROTECTION GUIDANCE

29 May 2020

We set out below a high-level summary of recent guidance issued by regulators across the world, addressing the use of personal data for specific purposes relating to the Covid-19 coronavirus, and the application of data protection laws in the current environment.

The high-level summaries included reflect the key messages as at 29 April 2020 except as otherwise specified against the jurisdiction/location (see contents list, for example, UK, France, Spain, Netherlands, Hungary, certain European institutions and International organisations). This week we have further updated New Zealand (OPC, CERTNZ), Australia (Government, OAIC, ACSC) and the Global Privacy Assembly reflecting the latest publications as at 28 May 2020. New guidance and advice is being issued all the time and so we will continue to update this overview with further summaries of the latest publications.

Africa	5
South Africa	5
Americas	9
Argentina.....	9
Canada	10
Canada (Alberta).....	14
Canada (Quebec).....	16

Canada (British Columbia)	17
Mexico	17
Peru	24
USA	28
APAC.....	51
Australia [Updated as at 28 May 2020].....	51
China	70
Hong Kong (SAR), China	71
India	78
Japan	90
New Zealand [Updated as at 28 May 2020].....	92
Philippines.....	106
Singapore.....	109
South Korea	110
Europe.....	110
European Parliament [Updated as at 21 May 2020]	110
European Commission [Updated as at 21 May 2020].....	117
European Data Protection Board (EDPB).....	136
European Data Protection Supervisor (EDPS) [Updated as at 21 May 2020]	155
European Banking Authority (EBA)	166
European Insurance and Occupational Pensions Authority (EIOPA).....	170

EUROPOL	171
Computer Emergency Response Team for the EU Institutions (CERT EU)	172
EU Agency for Cybersecurity (ENISA) [Updated as at 21 May 2020]	172
European Union Agency for Fundamental Rights (EU FRA)	184
Austria.....	185
Belgium.....	187
Croatia	193
Czech Republic.....	194
Denmark	198
Estonia.....	209
France [Updated as at 21 May 2020]	211
Finland	247
Germany	249
Greece	267
Hungary [Updated as at 21 May 2020]	273
Iceland	276
Ireland.....	278
Italy	286
Latvia	295
Luxembourg.....	298
Netherlands [Updated as at 14 May 2020]	299
Norway.....	326

Poland.....	332
Romania	337
Russian Federation	338
Spain [Updated as at 21 May 2020]	342
Sweden.....	359
UK [Updated as at 14 May 2020]	372
Middle East.....	424
Israel.....	424
United Arab Emirates (Abu Dhabi)	431
United Arab Emirates (Dubai).....	432
International.....	436
International Conference of Information Commissioners (ICIC) [Updated as at 21 May 2020].....	436
G20 ministers for Digital Economy [Updated as at 21 May 2020]	436
Organisation for Economic Co-operation and Development (OECD).....	438
International Criminal Police Organisation (Interpol).....	443
Financial Action Task Force (FATF)	444
Council of Europe [Updated as at 21 May 2020]	446
Global Privacy Assembly (GPA) [Updated as at 28 May 2020].....	451

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
AFRICA					
South Africa	Information Regulator	3/4/20	<p>Information Regulator issues guidance on the processing of personal information in relation to the Covid-19 coronavirus pandemic</p> <p>The Information Regulator issued guidance on the processing of personal information in the management and containment of the Covid-19 coronavirus. The guidance is intended both to outline the obligations on organisations to protect an individual's right to privacy, as well as to provide guidance to organisations on limiting this right to privacy when processing personal information in the context of containing the Covid-19 coronavirus pandemic.</p> <p>The guidance confirms that organisations must adhere to a number of conditions and principles when processing personal information, including ensuring accountability, maintaining a lawful basis of processing, retaining personal information only for as long as reasonably practicable, ensuring personal information is complete, accurate and not misleading, and implementing and maintaining policy</p>	<p>The press release is available here.</p> <p>The guidance is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-public authorities</p> <p>Data processing-location data</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>documentation for processing activities in relation to the Covid-19 coronavirus.</p> <p>The guidance also comments on a number of issues, including:</p> <ul style="list-style-type: none"> • data subject consent – the Information Regulator confirms that an individual cannot withhold their consent to be tested for the Covid-19 coronavirus, and consent is not necessary to process personal information where such processing complies with a legal obligation of the processor, protects the data subject's legitimate interests, is necessary for the performance of a public law duty by a public body, or is necessary for pursuing the legitimate interests of the responsible party or a third party recipient of the personal information; • purpose limitation – the Information Regulator confirms that responsible parties must collect personal information of a data subject for a specific purpose, which in this context is to detect, contain and prevent the spread of Covid-19. Further processing of personal 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>information for purposes not compatible with the original purpose for which it was collected is allowed if necessary to prevent a serious and imminent threat to public safety or public health, or the life or health of an individual;</p> <ul style="list-style-type: none"> • sharing of location data – the Information Regulator confirms that electronic communication service providers must provide the Government with mobile location data for the purposes of tracking data subjects to manage the spread of Covid-19 coronavirus, though the Government may only process such data lawfully. Sharing location data for conducting mass surveillance of data subjects is also allowed, if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form; and • employee health information – the Information Regulator confirms that an employer can request information on an employee's health status (though any disclosed information must not be used to unfairly discriminate against the 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			employee) and can require an employee to undergo testing for the Covid-19 coronavirus.		
South Africa	Information Regulator	19/3/20	<p>Information Regulator publishes statement on importance of privacy laws in relation to the Covid-19 coronavirus</p> <p>The Information Regulator has issued a press release addressing both the importance of public access to information relating to the Covid-19 coronavirus pandemic and the right to privacy in the management and containment of the virus.</p> <p>The Information Regulator requests that the South African Government proactively discloses all information relating to the virus and engages with social media companies to ensure that information on all platforms is fact-checked. The Information Regulator also called upon state agencies to make information available regularly, such as cancelled flights in the case of airlines, in a form and language accessible to all South Africans.</p> <p>The Information Regulator clarifies that, although the South African Protection of Personal Information Act (POPIA) allows the processing of information for</p>	The press release is available here .	Data protection-general guidance Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>statistical or research purposes, health and testing centres must adhere to all provisions of POPIA.</p> <p>Finally, the Information Regulator explains that the current situation has increased the use of technologies such as shopping and banking online in order to minimise social contact. In light of this, public and private bodies should increase their cybersecurity measures to protect personal information.</p>		
AMERICAS					
Argentina	Argentinian Agency for Access to Public Information (AAIP)	11/3/20	<p>AAIP issues general guidance on processing personal data in relation to the Covid-19 coronavirus</p> <p>The AAIP's statement reiterates that health-related information is sensitive personal data, which enjoys a higher level of protection under the Personal Data Protection Act (the Act).</p> <p>The statement also notes that disclosing the identity of individuals with Covid-19 coronavirus requires an individual's consent under Article 5 of the Act.</p> <p>Healthcare institutions and health professionals may process and share patient data with each other, subject to professional secrecy. They will require</p>	The press release is available here (only in Spanish).	Data protection-general guidance Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			patient consent if they intend to use patient information for purposes other than medical treatment. The National Ministry of Health and provincial ministries are entitled to process health information without the consent of patients, as provided by law (Art. 5 and 11 of the Act).		
Canada	Office of the Privacy Commissioner of Canada (OPC)	17/4/20	<p>OPC publishes framework to assess privacy impact of public health measures</p> <p>The OPC published an assessment framework to assist governmental bodies assess and minimise the impact on privacy when implementing measures in response to the Covid-19 coronavirus pandemic</p> <p>The framework provides a summary of key privacy principles and key messages that should be considered by government authorities. The OPC identifies the following key principles (among others):</p> <ul style="list-style-type: none"> • legal authority – bodies must identify a legal authority in order to collect, use and disclose personal information; • necessity and proportionality – bodies should ensure any measures taken are necessary 	<p>The press release is available here.</p> <p>The framework is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and proportionate i.e. essentially evidence-based for a specific purpose;</p> <ul style="list-style-type: none"> • purpose limitation – bodies should not use personal data processed to alleviate the Covid-19 coronavirus pandemic for any other reason and should, in general, delete when the crisis ends; • de-identification and safeguarding – bodies should use de-identified or aggregated data wherever possible and be aware of the real risk of re-identification; • protection of the vulnerable – bodies should consider the unique privacy impacts of measures on vulnerable groups in society; • openness and transparency – bodies should provide clear and detailed information about new and emerging measures; • open data – bodies should carefully consider the benefits and risks of disclosing public datasets • oversight and accountability – any new measures or legislation specific to the Covid- 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>19 coronavirus pandemic should contain specific provisions for oversight and accountability-more not less than usual; and</p> <ul style="list-style-type: none"> time limitation – measures that are invasive on individual privacy should be time limited. 		
Canada	Office of the Privacy Commissioner of Canada (OPC)	20/3/20	<p>OPC issues guidance in relation to the Covid-19 coronavirus</p> <p>On 20 March 2020, the OPC published a general guidance document for organisations subject to federal Canadian privacy laws. The guidance provides an overview of the privacy legislation at the federal, provincial and territorial levels, and the relevant provincial and territorial privacy authorities which have released guidance on the Covid-19 coronavirus pandemic.</p> <p>The OPC outlines the circumstances under which a public and private organisation may generally collect, process and disclose personal data, including without the individual's consent, under the Privacy Act 1985 (in relation to federal government departments and agencies) and PIPEDA (in relation to private organisations).</p>	<p>The press release is available here.</p> <p>The online guidance is available here.</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The OPC notes that where federal and provincial governments may declare formal public emergencies, the powers to collect, use and disclose personal information may be extended. Normal privacy laws apply unless emergency legislation provides otherwise. Where an organisation relies upon any provisions under applicable privacy laws that authorise the processing and disclosure of personal information in a public health crisis, it must communicate the specific legislative authority for this processing to the affected individuals.</p>		
Canada	Canadian Centre for Cyber Security (CCCS)	15/3/20	<p>Canadian Centre for Cyber Security issues guidance on Cyber Hygiene in relation to the Covid-19 coronavirus</p> <p>The CCCS published guidance on how individuals can protect themselves against phishing attempts. The guidance follows an increase in reports of phishing attempts referencing the Covid-19 coronavirus and impersonating official health agencies. The guidance reminds individuals to be wary of malicious emails and attachments.</p>	The guidance is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Canada (Alberta)	Office of the Information and Privacy Commissioner of Alberta (Alberta OIPC)	23/4/20	<p>Alberta OIPC issues statement on government tracing application</p> <p>The Alberta OIPC issued a statement in response to the Government of Alberta's announced proposal for a contact tracing application.</p> <p>The Alberta OIPC notes that, in order to build public trust, the application should clearly outline the types of personal data processed, the purposes of processing, and the circumstances in which the data will be disclosed and retained.</p> <p>The statement confirmed that the Government of Alberta has committed to conducting a privacy impact assessment and the OIPC will review the same.</p>	The statement is available here .	Mobile apps and new technology
Canada (Alberta)	Office of the Information and Privacy Commissioner of Alberta (Alberta OIPC)	19/3/20	<p>Alberta OIPC issues notice on conducting PIAs during the Covid-19 coronavirus pandemic</p> <p>The Alberta OIPC issued a notice on the obligation of health custodians to conduct a privacy impact assessment (PIA) during the Covid-19 coronavirus pandemic.</p> <p>Under section 64 of the Alberta Health and Information Act, health custodians are obliged to complete a PIA in relation to any processing of</p>	The notice is available here .	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>individually identifying health data that may impact an individual's privacy. The Alberta OIPC confirmed that health custodians remain obliged to conduct a PIA, even during a public health emergency, and the Alberta OIPC does not have authority to relax or disregard the requirements.</p> <p>However, acknowledging the practical challenges facing health custodians (such as in completing a PIA), the Alberta OIPC has requested that health custodians (at the very least) notify the Alberta OIPC via email where it is considering new administrative practices which may impact on an individual's privacy and include a description of the practices and any safeguards in place.</p> <p>Where a custodian is introducing new measures that may impact an individual's privacy, the notice highlights the need for health custodians to inform individuals of any heightened risks and to implement reasonable safeguards in the circumstances.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Canada (Quebec)	Quebec's Commission on Access to Information (CAI)	14/4/20	<p>CAI publishes comments on privacy issues in new technologies responding to the Covid-19 coronavirus pandemic</p> <p>The CAI published a summary document providing a high-level overview of the privacy issues arising from new technologies developed in response to the Covid-19 coronavirus pandemic. The CAI notes that such technologies typically involve disclosure of geolocation data, contact tracking applications, and infection tracking technology.</p> <p>The document provides a summary of the privacy issues to be considered before such technologies are used in Quebec. The CAI highlights the importance of supervision, reporting and independent external control of the technologies, and notes that any use and disclosure of personal information must be limited and subject to specific rules in relation to biometric and geolocation data.</p>	<p>The press statement is available here (only in French).</p> <p>The summary document is available here (only in French).</p>	<p>Mobile apps and new technology</p> <p>Data processing-location data</p>
Canada (Quebec)	Quebec's Commission on Access to Information (CAI)	17/3/20	<p>CAI issues guidance on data processing in relation to Covid-19 coronavirus pandemic</p> <p>The CAI statement notes that under Quebec data protection law (the Act Respecting the Protection of Personal Information in the Private Sector), public</p>	<p>The statement is available here (only available in French).</p>	<p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			bodies and private companies are required to respond to data subject requests within 30 days. However, as measures to limit the Covid-19 coronavirus pandemic may prevent companies and organisations from responding within this time frame, the CAI note that (where this deadline is missed) the law considers such requests to be refused and the data subject has 30 days to file an appeal with the CAI.		
Canada (British Columbia)	Office of the Information and Privacy Commissioner for British Columbia (OIPC)	16/3/20	OIPC issues brief statement on Covid-19 coronavirus The OIPC statement notes that British Columbia's Provincial Health Officer has broad authority to collect and use personal information in the public interest during a pandemic. The OIPC suggests that public and private organisations should contact it if unsure of their responsibilities or authority to collect and process personal information.	The statement is available here .	Data protection-general guidance
Mexico	Mexican National Institute of Access to Information and Data Protection (INAI)	7/4/20	INAI issues statement on use of geolocation data in light of the Covid-19 coronavirus pandemic The President of INAI, Francisco Javier Acuña Llamas, issued a brief statement addressing the INAI's own role in light of the Covid-19 coronavirus	The statement is available here (only in Spanish).	Data protection-regulator approach Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>pandemic and the use of geolocation data. The statement confirms that the INAI is still operational and closely observing the flows of urgent and important information that need to reach the healthcare sector.</p> <p>The INAI further emphasises that it is diligently monitoring the protection of individuals' personal information, in particular those who have been diagnosed with Covid-19 coronavirus. If geolocation data is to be used in Mexico to control the spread of the pandemic (as was seen in Korea), the INAI confirms that authorities must follow the protocols, specific channels and situations verified by the INAI.</p>		
Mexico	Mexican National Institute of Access to Information and Data Protection (INAI)	8/4/20	<p>INAI publishes recommendations on remote working related to Covid-19 coronavirus pandemic</p> <p>The INAI recommends that organisations establish physical, administrative and technical measures to comply with the security and confidentiality obligations applicable to protection of personal data during remote working that is part of measures to contain the Covid-19 coronavirus pandemic.</p>	The guidance is available here (only in Spanish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The INAI recommendations include, amongst others:</p> <ul style="list-style-type: none"> • using company computer equipment and tools and ensuring that personal devices used for remote work have up-to-date firewall, antivirus and intrusion prevention software; • avoiding use of public or free access networks; • formatting external storage devices; • preventing infection of devices with malware by enabling antivirus scans or prohibiting downloads on these devices; • ensuring that appropriate security measures are in place; • using only official electronic communication channels (office email or company instant messaging programs) installed on company devices to send and receive confidential information; • using secure access control measures, such as strong passwords, multi-factor authentication and encryption to restrict 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>access to the device and reduce risk of compromising the security of personal data;</p> <ul style="list-style-type: none"> • turning off or disconnecting computers from private networks when not in use, especially if they are connected to corporate systems; • encrypting all storage devices that contain confidential information or personal data. 		
Mexico	Mexican National Institute of Access to Information and Data Protection (INAI)	2/4/20	<p>INAI releases statement requesting extreme caution on use of personal data of Covid-19 coronavirus patients</p> <p>The INAI statement notes that public and private entities that handle personal data of individuals infected by the Covid-19 coronavirus should use strict administrative, physical and technical measures to avoid any loss, destruction, theft or improper use of patients' personal data, and urges compliance with the principles, duties and obligations established in Mexico's data protection laws.</p> <p>In order to prevent security risks and respect privacy of people affected by the spread of the Covid-19 coronavirus, the INAI has formulated a number of</p>	The statement is available here (only in Spanish).	Data protection-general guidance Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>recommendations for personal data processing in this context, including:</p> <ul style="list-style-type: none"> • measures implemented in response to the pandemic that involve processing personal health data must be necessary and proportional, and follow the instructions of the health and other competent authorities; • only the minimum necessary personal data that are necessary for achieving the purpose of containment measures should be collected; • personal data collected to prevent or contain the spread of coronavirus should not be used for other purposes; • the confidentiality of sensitive data must be protected to avoid harm to or discrimination against the affected individual; • when communicating within the organisation about the possibility of Covid-19 coronavirus infection in the workplace, organisations should not identify any infected individual; • the identity of individuals affected by the Covid-19 coronavirus should not be 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>disclosed. If personal data disclosure to health authorities is required, this must be clearly documented, substantiated and carried out with due appropriate security measures;</p> <ul style="list-style-type: none"> • organisations must determine the retention period for personal data related to Covid-19 coronavirus cases, as well as the mechanisms that will be used to securely delete this data, taking into account applicable sector regulations; and • capturing and disseminating images or videos of Covid-19 coronavirus patients or deceased persons must be avoided. 		
Mexico	Mexican National Institute of Access to Information and Data Protection (INAI)	15/4/20	<p>INAI issues press release confirming suspension of certain regulatory deadlines due to the Covid-19 coronavirus pandemic</p> <p>The INAI announced on 20 March 2020 that it has suspended the terms and deadlines established for information requests, complaints and sanctions due to the emergency in Mexico caused by the spread of the Covid-19 coronavirus. The suspension applies from</p>	<p>The press release of 20 March 2020 is available here (only in Spanish).</p> <p>The press release extending the suspension until 30</p>	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>23 March 2020 until 17 April 2020. This term has been further extended until 30 April 2020.</p> <p>The INAI also set out the actions it will take to ensure the disclosure and publicity of relevant, reliable, truthful and timely information to Mexican citizens at this time, through various digital channels. This includes maintaining a dialogue with the health sector to identify the relevant information.</p>	<p>April 2020 is available here (only in Spanish).</p>	
Mexico	Mexican National Institute of Access to Information and Data Protection (INAI)	13/3/20	<p>INAI issues recommendations regarding data processing in relation to the Covid-19 coronavirus</p> <p>The INAI statement provides recommendations for organisations and the general population when processing personal data relating to the Covid-19 coronavirus. In particular, the INAI reiterates that any processing of personal data must comply with the principles, duties and obligations of data protection law, other than in exceptional cases which are provided for in law.</p> <p>The statement also notes that security measures should be implemented and the confidentiality of personal data must be protected to avoid harm or discrimination to the affected individuals. By way of example, the INAI recommends that individuals are</p>	<p>The statement is available here (only in Spanish).</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			not identified in any communication about the presence of the Covid-19 coronavirus in the workplace.		
Peru	Peruvian Data Protection Authority (APDP)	18/4/20	<p>APDP issues statement on emergency decree and the use of geolocation data in relation to Covid-19</p> <p>The statement on Supreme Decree No. 70-2020-PCM and the use of geolocation data for Covid-19 coronavirus cases (the Statement) notes that entities managing emergency telephone numbers have access to the personal data of individuals who report Covid-19 coronavirus symptoms, and that data must be anonymised before being sent to other entities for the fulfilment of their duties.</p> <p>The Statement also explains that, where there are cases of suspected or confirmed Covid-19 coronavirus, the entities managing emergency telephone numbers will have access to geolocation history of the device from which the call is made. The APDP stressed that the use of this data must only be for the intended purposes, and entities must put in place technical, organisational and legal measures to safeguard the confidentiality, integrity and availability</p>	<p>The Statement is available here.</p> <p>The Decree itself here. (both only in Spanish)</p>	Data processing- location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			of the data until its deletion which should be when the Covid-19 coronavirus state of emergency has ended.		
Peru	Presidency of the Council of Ministers (the Presidency)	3/4/20	<p>Presidency of the Council of Ministers announces launch of Covid-19 coronavirus app</p> <p>The Presidency announced the launch of a Covid-19 coronavirus app "Perú en tus manos" which allows self-assessment of Covid-19 coronavirus infection risk and information on high-risk areas. It also allows users to share their location so that they may receive assistance from health professionals and alerts about risk areas in Peru.</p> <p>The announcement also discussed more detail of the mobile app functionality, noting that, on download, individuals will receive a validation code through a text message to certify their registration and identification and that, if the app determines a user to be at risk, it will notify the user of this and request the user's personal data, such as their ID and phone number (amongst others).</p> <p>The Ministry of Health will contact the individuals to follow up on their case and provide recommendations to prevent contagion.</p>	The press release is available here (only in Spanish).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Peru	Peruvian Data Protection Authority (APDP)	21/3/20	<p>APDP urges media to comply with data protection legislation when disclosing names and images of Covid-19 coronavirus patients</p> <p>On 21 March 2020, the APDP confirmed that media outlets may only disclose the names and images of patients with the Covid-19 coronavirus with the individual's prior written consent. Reiterating previous comments made on 12 March 2020, the APDP noted that failure to obtain such consent may violate the Law for Personal Data Protection 2011 (Law No. 29733).</p> <p>The APDP highlights that personal data of Covid-19 coronavirus patients may only be used without prior written consent by authorised health officials and in the implementation of public health measures.</p> <p>However, the APDP notes that media outlets may disclose information that does not, and would not enable others to, identify individuals, such as the number of patients with the Covid-19 coronavirus and the age and gender of the individuals.</p>	The press release is available here (only in Spanish).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Peru	Peruvian Data Protection Authority (ANPD)	12/3/20	<p>ANPD issues recommendations on data protection of individuals with the Covid-19 coronavirus</p> <p>The ANPD released recommendations emphasising that sensitive data related to individuals who have contracted the Covid-19 coronavirus can only be disclosed upon their free, prior, express, unambiguous and informed consent, which should be provided in writing.</p> <p>The ANPD warned that because sharing personal data related to the Covid-19 coronavirus can cause moral and psychological harm to individuals, it is not recommended to disclose a patient's name, address, photographs or clinical history (including through publication on social media) without patient consent. Confidential medical information provided as part of the doctor-patient relationship cannot be disclosed, even after the professional relationship is terminated.</p> <p>Healthcare providers should implement necessary security measures in relation to medical data and may only disclose confirmed cases to the Ministry of Health.</p>	The guidance is available here (only in Spanish).	<p>Data protection-general guidance</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
USA	The Department of Health & Human Services (HSS) Office for Civil Rights (OCR)	9/4/20	<p>OCR announces enforcement discretion during the Covid-19 coronavirus outbreak regarding Community-Based Testing Sites</p> <p>The OCR issued a notification stating that enforcement discretion and penalty waivers for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules will apply to covered entities and business associates in connection with the good faith participation in the operation of Covid-19 coronavirus community-based testing sites (CBTS) (including mobile, drive-through, or walk-up sites that only provide Covid-19 coronavirus specimen collection or testing services to the public).</p> <p>The notification of enforcement discretion has retroactive effect from 13 March 2020 and will remain in place until the Secretary of Health and Social Services declares the public health emergency no longer exists or until the expiry of the declared public health emergency.</p>	<p>The press release is available here.</p> <p>The notification is available here.</p>	<p>Data protection-regulator approach</p> <p>Data protection-general guidance</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>OCR encourages such healthcare providers to implement reasonable safeguards to protect the privacy and security of individuals' PHI including:</p> <ul style="list-style-type: none">• using/disclosing minimum PHI necessary except when disclosing for treatment;• setting up canopies/opaque barriers at a CBTS to provide privacy;• controlling traffic to create adequate distancing to minimise risk of overhearing;• establishing a "buffer zone" to prevent media access and posting signs prohibiting filming;• using secure technology to record and transmit electronic PHI;• posting a Notice of Privacy Practices, or information about how to find the NPP online, if applicable, in a place that is readily viewable by individuals who approach a CBTS.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
USA	Cybersecurity and Infrastructure Security Agency (CISA)	8/4/20	<p>CISA issues teleworking guidance on securing networks and cloud environments used by the federal workforce</p> <p>CISA has issued Trusted Internet Connections 3.0 Interim teleworking guidance for agencies and federal workers in relation to securing connections to private networks and cloud environments as greater numbers telework and use collaboration tools. Connections to the public internet will continue to route through the National Cybersecurity Protection System EINSTEIN.</p> <p>Guidance:</p> <ul style="list-style-type: none"> • suggests security capabilities for agencies to consider when creating/expanding teleworking platforms; • highlights interaction with other TIC guidance; • requires that agencies should ensure appropriate data sharing is maintained with Agency Security Operations Centers; • requires that agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant 	<p>The press release is available here.</p> <p>The guidance is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>information will need to be provided to CISA for cybersecurity analytical purposes;</p> <ul style="list-style-type: none"> • informs agencies that the interim guidance provided under Agency Teleworker Option 3 provides additional temporary relief with additional security patterns. <p>CISA encourages vendors to map cybersecurity capabilities in their services to the interim guidance, though agencies should continue to assess vendors through their standard due diligence and risk management processes.</p> <p>The guidance is short term and will be phased out, though features will be integrated in longer term guidance.</p> <p>Though the guidance is applicable to federal agencies, the risks and issues covered can be more generally applicable to private organisations.</p>		
USA	Federal Trade Commission (FTC)	27/3/20	<p>FTC warns nine companies for assisting and facilitating Covid-19 coronavirus scams</p> <p>FTC warned nine Voice over Internet Protocol (VoIP) service providers and other companies assisting and</p>	<p>The press release is available here.</p> <p>The letters are available here.</p>	Data protection – regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>facilitating illegal telemarketing and robocalls in connection with the Covid-19 coronavirus pandemic.</p> <p>The FTC cited violations of the Telemarketing Sales Rule (TSR), flagged past enforcement actions taken against VoIP providers for knowingly transmitting robocalls and noted that the FTC will pursue enforcement if companies continue to assist telemarketers in violation of the TSR.</p> <p>The FTC required a response describing the specific actions the company has taken to ensure its services are not being used in Covid-19 coronavirus robocall schemes.</p>		
<p>USA</p>	<p>The Department of Health & Human Services (HSS) Office for Civil Rights (OCR)</p>	<p>2/4/20</p>	<p>OCR announces enforcement discretion during the Covid-19 coronavirus outbreak</p> <p>The OCR issued a notification stating that healthcare providers and their business associates who, in good faith, disclose protected health information for public health and health oversight activities during the Covid-19 coronavirus outbreak that would ordinarily breach provisions in the 1996 Health Insurance Portability and Accountability Act (HIPAA) will be subject to enforcement discretion and the waiving of potential penalties by the OCR.</p>	<p>The press release is available here. The notification is available here.</p>	<p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>However, the OCR emphasises that the enforcement discretion does not extend to all prohibitions under the HIPAA. For example, business associates remain liable for complying with the requirements on the confidentiality, integrity and availability of electronic protected health information and ensuring secure transmission of health information to the public health authority or health oversight agency.</p> <p>The notification of enforcement discretion will remain in place until the Secretary of Health and Social Services declares the public health emergency no longer exists or until the expiry of the declared public health emergency.</p>		
USA	The Department of Health & Human Services (HSS) Office for Civil Rights (OCR)	24/3/20	<p>OCR issues guidance on disclosure of protected health information about individuals exposed to Covid-19 coronavirus</p> <p>OCR issued guidance on the disclosure of protected health information (PHI) about individuals who have been infected with or exposed to Covid-19</p>	<p>The press release is available here.</p> <p>The guidance is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>coronavirus, in a way that is compliant with the HIPAA Privacy Rule:</p> <p>(a) by Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities;</p> <p>(b) to law enforcement, paramedics, other first responders and public health authorities.</p> <p>According to the guidance, covered entities may disclose PHI, without HIPAA authorisation, in circumstances including:</p> <ul style="list-style-type: none"> • when needed for the provision of treatment; • when required by law; • to notify a public health authority in order to prevent or control spread of disease; • when first responders may be at risk of infection; • when the disclosure of PHI to first responders is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> when responding to a request for PHI by a correctional institution or law enforcement official having lawful custody of an inmate or other individual and meeting certain further criteria. <p>Covered entities must take reasonable steps to limit disclosure or use of PHI to the minimum necessary to achieve the purpose for the disclosure.</p> <p>Guidance provides further clarification, examples and discussion.</p>		
USA	US Equal Employment Opportunities Commission (EEOC)	21/3/20	<p>EEOC updates its Pandemic Preparedness guidance to address Covid-19 coronavirus</p> <p>The EEOC has updated its Pandemic Preparedness in the Workplace and the Americans With Disabilities Act guidance (Pandemic Guidance) with relevant examples and information to help employers implement strategies to navigate the impact of the Covid-19 coronavirus.</p> <p>The EEOC clarifies that anti-discrimination laws (including Americans with Disabilities Act, the ADA) and Rehabilitation Act rules continue to apply but do not "interfere with or prevent employers from following the guidelines and suggestions made by the CDC or</p>	<p>The press release is available here.</p> <p>The guidance is available here.</p>	Data processing-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>state/local public health authorities about steps employers should take regarding COVID-19".</p> <p>Amongst other things, Pandemic Guidance includes clarification that:</p> <ul style="list-style-type: none"> • employers may make enquiries about availability to work in a pandemic as long as they are not disability-related (detail provided) and the question is structured so that the employee gives one answer of "yes" or "no" to the whole question without specifying the factor(s) that apply to him. The answer need not be given anonymously; • ADA-covered employers should not generally ask asymptomatic employees to disclose whether they have a medical condition that could make them especially vulnerable to complications. If an employee voluntarily discloses this information, the employer must keep this information confidential. ADA-covered employers may make disability-related enquiries or require medical examinations of asymptomatic employees to identify those at higher risk if the employer has 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>sufficient objective information from public health advisories to reasonably conclude that employees will face a direct threat if they contract the pandemic virus.</p> <p>In addition, the press release replicates a number of FAQs from the Pandemic Guidance, clarifying, amongst other things, that:</p> <ul style="list-style-type: none"> • during a pandemic, ADA-covered employers may ask employees who call in sick if they are experiencing symptoms of the Covid-19 coronavirus, but must maintain all information about employee illness as a confidential medical record in compliance with the ADA; • because the Centers for Disease Control and Prevention and state/local health authorities have acknowledged community spread of Covid-19 coronavirus and issued precautions, employers may measure employees' body temperature, despite this being considered a medical examination; • employers may require a doctor's certificate of fitness to work following a Covid-19 coronavirus related absence; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> employers may screen job applicants for symptoms of the Covid-19 coronavirus after making a conditional job offer, as long as they do so for all employees entering the same type of job; medical exams are permitted after an employer has made a conditional offer of employment and this may include taking the individual's temperature. 		
USA	Federal Communications Commission (FCC)	20/3/20	<p>FCC issues a declaratory ruling regarding Covid-19 coronavirus and Telephone Consumer Protection Act</p> <p>The FCC issued a declaratory ruling (the Ruling) addressing compliance with the Telephone Consumer Protection Act of 1991 (TCPA) in the context of Covid-19 coronavirus.</p> <p>The Ruling specifies, amongst other things, that the Covid-19 coronavirus constitutes an "emergency" under the TCPA and as such hospitals, healthcare providers, state and local health officials, and other government officials may lawfully communicate information about the Covid-19 coronavirus and mitigation measures without breaching the law.</p>	The ruling is available here .	Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Ruling clarifies that the content of the call must be solely informational, made necessary because of the Covid-19 coronavirus outbreak, and directly related to the imminent health or safety risk arising out of the Covid-19 coronavirus outbreak.</p> <p>In general, the TCPA and the FCC's rules prohibit auto-dialled, pre-recorded, or artificial voice calls to wireless telephone numbers and other specified recipients (both voice calls and text messages, including SMS if the call is made to a telephone number assigned to such a service). The exception to this is where calls are made for an "emergency purpose", i.e. calls made necessary in any situation affecting the health and safety of consumers, in "instances [that] pose significant risks to public health and safety, and [where] the use of pre-recorded message calls could speed the dissemination of information regarding... potentially hazardous conditions to the public".</p> <p>The Ruling provides examples of communications that would fall within the scope of the exception and examples of communications that would not. For example, calls that contain advertising or telemarketing of services do not constitute calls made</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			for an "emergency purpose" such as advertising a commercial grocery delivery service, or selling or promoting health insurance, cleaning services, or home test kits.		
USA	The Department of Health & Human Services (HSS) Office for Civil Rights (OCR)	20/3/20	<p>OCR issues further guidance on telehealth remote communications following its Covid-19 coronavirus Notification of Enforcement Discretion</p> <p>The OCR has issued a set of frequently asked questions (FAQs) regarding telehealth remote communications as a follow up to its notification of enforcement discretion under HIPAA of 17/3/20 (the Notification, see below).</p> <p>Amongst other things, the FAQs clarify that:</p> <ul style="list-style-type: none"> • telehealth is "the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, and public health and health administration"; • whilst the Notification applies to healthcare providers covered by HIPAA that provide telehealth services during the Covid-19 	<p>The press release is available here.</p> <p>The FAQs are available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>coronavirus emergency, the enforcement discretion does not apply to health insurance companies that pay for telehealth services;</p> <ul style="list-style-type: none"> • applicable healthcare providers will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur in good faith in relation to the provision of telehealth services during the Covid-19 coronavirus emergency; • the Notification does not affect the application of the Rules to other areas of healthcare outside the Covid-19 coronavirus emergency; • the OCR expects telehealth to be conducted in private settings, (e.g. doctor in a clinic connecting to a patient at home) and not in public or semi-public settings, absent patient consent or exigent circumstances; • if telehealth cannot be provided in a private setting, healthcare providers should continue to implement reasonable HIPAA safeguards to limit incidental uses or disclosures of protected health information (e.g. lowered voices, not using speakerphone, or recommending that 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the patient move to a reasonable distance from others during the discussion);</p> <ul style="list-style-type: none"> examples of "bad faith" use of telehealth communications include (amongst others) use that is an intentional invasion of privacy and use where there is a further use or disclosure of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (e.g. sale of the data, or use of the data for marketing without authorisation); the OCR will issue a notice when it will no longer exercise its enforcement discretion. 		
USA	National Institute of Standards and Technology (NIST)	19/3/20	<p>NIST releases a bulletin regarding telework security</p> <p>NIST published an Information Technology Laboratory Bulletin on Telework Security (the Bulletin) as millions of Americans transitioned to their homes to continue to work.</p> <p>The Bulletin is based on the 2016 NIST Special Publication (SP) 800-46Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security and summarises some of the</p>	<p>The press release is available here.</p> <p>The Bulletin is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>key recommendations. Whilst it does not specifically reference Covid-19 coronavirus, the publication is obviously relevant as more employees look to work from home in the context of Covid-19 coronavirus mitigation steps.</p> <p>The Bulletin includes information regarding:</p> <ul style="list-style-type: none"> • development and enforcement of a telework security policy, (e.g. tiered levels of remote access); • multi-factor authentication for enterprise access; and • security of telework client devices. <p>NIST has also flagged the Telework Cybersecurity section on the CSRC homepage, noting that it will be updated as new NIST cybersecurity and privacy resources for telework become available. The site currently includes resources such as:</p> <ul style="list-style-type: none"> • two Cybersecurity Insights blog posts on 1) Telework Security Basics and 2) Preventing Eavesdropping and Protecting Privacy on Virtual Meetings; and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> NIST Special Publications that support telework, mobile device security, and Transport Layer Security (TLS) use for virtual private networks (VPNs). 		
USA	The Department of Health & Human Services (HSS) Office for Civil Rights (OCR)	17/3/20	<p>OCR intends to use discretion in enforcing HIPAA violations related to video chat services in context of the Covid-19 coronavirus pandemic</p> <p>OCR published a notification stating that it would use discretion when enforcing violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) against healthcare providers in the context of patient communications during the Covid-19 coronavirus outbreak.</p> <p>Some of the technologies and the manner in which they are used by healthcare providers to communicate with patients during the Covid-19 coronavirus outbreak may not fully comply with the requirements of the HIPAA Rules (including lack of business associate agreements with providers of video technology products). Therefore, discretion will be exercised and penalties not imposed in relation to the use of non-public facing communications apps, such as Apple FaceTime, Facebook Messenger video</p>	<p>The press release is available here.</p> <p>The notification is available here.</p>	<p>Cybersecurity and information security</p> <p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>chat, Google Hangouts video, or Skype, where they are used in good faith for remote healthcare or diagnostic purposes.</p> <p>Importantly, the services provided using these methods need not be directly related to the Covid-19 coronavirus.</p> <p>This exercise of discretion does not apply to use of public facing apps such as Facebook Live, Twitch, TikTok, or similar.</p>		
USA	<p>The Cybersecurity and Infrastructure Security Agency (CISA)</p> <p>The U.S. Department of Homeland Security (DHS)</p> <p>The UK National Cyber Security Centre (UK NCSC)</p>	5/5/20	<p>The UK NCSC, the US CISA and DHS issue a joint warning of advanced persistent threat (APT) groups targeting healthcare bodies, pharmaceutical companies, and medical research organisations, among others.</p> <p>The latest warning follows a joint advisory publication issued on 8 April regarding cyber criminal exploitation of the Covid-19 coronavirus outbreak for their own personal gain (see later in this overview).</p> <p>The current alert highlights ongoing activity by APT groups against organisations involved in both national and international Covid-19 coronavirus responses, in particular pharmaceutical companies, research organisations, and local government, targeting</p>	<p>The NCSC news report and alert are available here and here.</p> <p>The CISA press release is available here.</p> <p>The CISA alert is available here.</p> <p>The joint advisory is available here.</p>	Cybersecurity and Information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>organisations to collect bulk personal information, intellectual property and intelligence that aligns with national priorities.</p> <p>The alert describes some of the methods APTs are using to target organisations. For example, ‘password spraying’ campaigns against healthcare bodies and medical research organisations (where the attacker tries a single and common password against many accounts before moving on to try a second password etc) and scanning external websites of targeted companies for vulnerabilities in unpatched software, taking advantage of vulnerabilities such as those in Virtual Private Network (VPN) products from certain vendors.</p> <p>The joint advisory report goes on to describe a number of mitigations including:</p> <ul style="list-style-type: none"> • updating Virtual Private Networks, network infrastructure devices, and devices being used to remotely access the work environment with the latest software patches and configurations; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • using modern systems and software with better in-built security; • using multi-factor authentication to reduce the impact of passwords being compromised; • protecting the management interfaces of critical operating systems; • setting up security monitoring systems; and • reviewing and refreshing incident management processes. <p>The advisory directs reader to a number of existing guidance documents of both the UK NCSC and the US CISA. The alert states that the NCSC and CISA will continue to investigate activity linked to APT actors.</p>		
USA	The US Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (US CISA)	8/4/20	<p>UK NCSC and the US CISA publish a joint advisory on malicious cyber activity exploiting the Covid-19 coronavirus pandemic</p> <p>The UK NCSC and the US CISA published a joint advisory with an overview of malicious cyber activity related to the Covid-19 coronavirus pandemic. The advisory provides information on exploitation by cybercriminal and advanced persistent threat (APT)</p>	<p>The press statement of the US CISA is available here.</p> <p>The press statement of the UK NCSC is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
	The UK National Cyber Security Centre (UK NCSC)		<p>groups, includes a non-exhaustive list of indicators of compromise for detection of attacks and practical advice on mitigating related risks.</p> <p>The advisory notes that APT groups and cybercriminals are actively using the pandemic for commercial gain, deploying various threats, including:</p> <ul style="list-style-type: none"> • phishing and malware distribution, while using the subject of coronavirus or Covid-19 as a lure; • registration of new domain names containing wording related to Covid-19 or coronavirus; and • attacks against newly deployed remote access and teleworking infrastructure, by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. <p>Recommendations for organisations include:</p> <ul style="list-style-type: none"> • using passwords or "waiting room" features for online meetings to control admittance of participants; 	The advisory is available here .	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • managing screen-sharing options when using communication platforms for online meetings; • ensuring teleworking policies address physical and information security requirements; • planning for successful phishing attacks; and • educating employees in identifying and reporting suspected phishing emails. <p>The advisory also identifies key online resources published by the UK NCSC and US CISA in relation to mitigating risk online, including:</p> <ul style="list-style-type: none"> • CISA guidance for defending against Covid-19 cyber scams; • CISA insights on risk management for Covid-19, with guidance for executives regarding physical, supply chain and cybersecurity issues; • NCSC guidance to help spot, understand and deal with suspicious messages and emails, guidance on phishing for organisations and cybersecurity professionals, and other materials. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
USA	Cybersecurity and Infrastructure Security Agency (CISA)	13/3/20	<p>CISA issues guidance on VPN security and working from home in the context of Covid-19 coronavirus</p> <p>The CISA published an alert on VPN security and working from home. In particular, the alert highlights the need to:</p> <ul style="list-style-type: none"> • ensure VPNs and network infrastructure devices have the latest security patches and configurations; • educate employees regarding increased likelihood of phishing attempts; • ensure that IT security personnel increase remote-access cybersecurity tasks (e.g. log review, attack detection, and incident response and recovery); and • implement multi-factor authentication. 	The alert is available here .	Cybersecurity and information security
USA	Financial Industry Regulatory Authority (FINRA)	9/3/20	<p>FINRA releases a regulatory notice on Covid-19 coronavirus business continuity planning, guidance and regulatory relief</p> <p>The FINRA released a regulatory notice on Pandemic-Related Business Continuity Planning, Guidance, and Regulatory Relief. Amongst other</p>	The notice is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>things, as part of pandemic preparedness, the notice highlights that firms should consider the increased threat of cyber events (e.g. systems being compromised through phishing attacks), due to the use of remote offices or telework arrangements.</p> <p>The notice identifies steps that may mitigate risk such as ensuring that VPN and remote access systems have up-to-date security patches, ensuring system entitlements are current, and using multi-factor authentication and communication/training regarding cyber risks.</p>		
APAC					
Australia [Updated as at 28 May 2020]	Australian Government	15/5/20	<p>Australia passes a law on COVIDSafe app privacy protections</p> <p>Privacy Amendment (Public Health Contact Information) Act, 2020 (the Act) is intended to help control the spread of Covid-19 coronavirus, amending the Privacy Act 1988 to provide stronger privacy protections for users of the COVIDSafe app and data collected through the app. and elevating provisions of the determination made under the Biosecurity Act 2015 to primary legislation.</p>	<p>The press release is available here.</p> <p>The Privacy Amendment (Public Health Contact Information) Act, 2020 is available here.</p> <p>The OAIC statement is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>More specifically, and amongst other things, the Act provides for the circumstances in which the COVIDSafe app can be used and the basis on which data can accessed, ie:</p> <ul style="list-style-type: none"> • by authorised state and territory health officials; • for contact tracing purposes and for the proper functioning, integrity and security of COVIDSafe and the National COVIDSafe Data Store; • after a user infected with the Covid-19 coronavirus consents to their encrypted data being uploaded. <p>Use of the COVIDSafe app is voluntary and the Act prohibits imposing mandatory use or data disclosure. It also provides for deletion of data on devices, deletion of data disclosed in error and deletion after a defined period.</p> <p>The Act allows de-identified statistics about the total number of registrations through the COVIDSafe app to be reported for transparency purposes.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Further, the Act provides for data storage requirements, specifying location of data retention (in Australia) and restrictions on disclosure outside of Australia.</p> <p>The Australian Privacy Act continues to apply to the personal information and the Act provides the Office of the Australian Information Commissioner (OAIC) with independent oversight powers. The OAIC may, amongst other things, investigate complaints, undertake assessments of compliance, investigate, assess and require cooperation of State and Territory health authorities in relation to their handling of COVIDSafe app data as well as the handling of personal information by the Commonwealth COVIDSafe app and National COVIDSafe Data Store.</p> <p>A breach involving the COVIDSafe app data will also constitute a Notifiable Data Breach under the Australian Privacy Act, subject to some flexibility and discretion of application by the OAIC.</p> <p>Criminal and civil penalties apply for any misuse (such as jail terms of up to five years, or a fine of AUD 63,000 per offence). It is a particular offence to coerce a person to use the app, to store or transfer COVIDSafe data to a country outside Australia, and to</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>decrypt app data. The OAIC can also order compensation to be paid to individuals who suffer from an interference with their privacy.</p> <p>In its statement regarding the Act on 14 May 2020, the OAIC welcomed the new law and commented that it is in keeping with its advice, in the Privacy Impact Assessment, that legislation provides the strongest form of protection to codify the privacy safeguards.</p> <p>The OAIC noted that it will monitor the handling of personal information in the COVIDSafe system and that “the oversight of the privacy protections passed today are a top priority for my office”.</p> <p>The OAIC will report on the performance and exercise of the OAIC's functions and powers, in accordance with the Act, in six months.</p>		
Australia	Australian Government	26/4/20	<p>Australian Government launches Covid-19 tracking app</p> <p>The Australian Department of Health has launched a new voluntary Covid-19 tracking app, COVIDSafe. The app:</p> <ul style="list-style-type: none"> uses Bluetooth technology to identify other nearby phones that have the app installed; 	<p>The Government press release is available here.</p> <p>The transcript from the Prime Minister's press conference is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • makes a secure 'digital handshake' that notes the date and time, distance and duration of the contact; • securely encrypts and stores the data on the user's phone, so that not even the user can access it; and • if an app user is diagnosed with the Covid-19 coronavirus and agrees to share their data, the relevant Australian state or territory public health officials will be able to access the user's information and that of any other individual in within their jurisdiction with whom the diagnosed user has had contact within 1.5 metres for 15 minutes or more. The health officials can then use that information for contact tracing purposes. <p>Information provided voluntarily through the app will only be accessible to authorised state or territory health officials. Any other access or use will be a criminal offence.</p> <p>Australian Prime Minister Scott Morrison confirmed that the information will be stored on an Amazon Web</p>	<p>The transcript from the Attorney General's interview is available here.</p> <p>The PIA is available here.</p> <p>The Department of Health response to the PIA is available here.</p> <p>The Government FAQs are available here.</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Services server in Australia in a nationally encrypted data store.</p> <p>The Attorney-General confirmed that the information will only be used for specific health purposes (i.e. contact tracing for Covid-19 coronavirus).</p> <p>An associated Privacy Impact Assessment was released on 25 April 2020, highlighting steps taken by the Australian Government to consider privacy by design, data minimisation and access limitations. The PIA includes recommendations amongst other things, to communicate with the public regarding the app’s function and purpose, minimise risk of loss of control of personal data and ensure voluntary consent.</p> <p>In the Department of Health’s response it confirmed that it will take note of the same, release source code and review effectiveness of the app.</p> <p>The Australian Government has produced a set of FAQs regarding the app, including the approach to privacy and security and this was last update on 29 May 2020.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Australia	Australian Government	20/4/20	<p>Government of Australia commits to releasing source code of Covid-19 coronavirus tracing apps and relevant privacy impact assessment</p> <p>The Australian Government has released a transcript of an interview given by The Hon Stuart Robert MP, Minister for the National Disability Insurance Scheme and Government Services, on the subject of Australia's Covid-19 coronavirus tracing app.</p> <p>In the interview, Robert attempts to encourage Australians to download the app by stating that it is held to a high standard of privacy and that the government will release the source code and relevant privacy impact assessment to demonstrate this commitment to privacy. Robert also emphasises that the app only replicates a manual tracing procedure and does not use geolocation data.</p>	The transcript of the interview is available here .	Mobile apps and new technology
Australia	Office of the Australian Information Commissioner (OAIC)	26/4/20	<p>OAIC releases statement on the Covid-19 coronavirus app, COVIDSafe</p> <p>The OAIC published a statement regarding the COVIDSafe app released by the Australian Government to track Covid-19 coronavirus, as further described in this overview above.</p>	<p>The statement is available here.</p> <p>The FAQs are available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The OAIC considered that important safeguards have been put in place to protect personal information collected through the app, and that it will have independent oversight of personal information handling by the app and the National COVIDSafe Data Store.</p> <p>The OAIC welcomed the publication of the PIA noting that it “provided transparency and accountability for the use of personal information, and supports community confidence in the app,”</p> <p>It confirmed that it will closely monitor progress of the app and associated legislation as it is developed.</p> <p>The OAIC has also published a set of FAQs for individuals in connection with use of the COVIDSafe app and the application of the Privacy Amendment (Public Health Contact Information) Act, 2020 (further described above in this overview).</p>		
Australia	Office of the Australian Information Commissioner (OAIC)	6/4/20	<p>OAIC publishes guidance on PIAs during the Covid-19 coronavirus outbreak</p> <p>The OAIC has published guidance on completing Privacy Impact Assessments (PIAs) in the context of the Covid-19 coronavirus pandemic, aiming to assist organisations regulated by the Privacy Act 1988 (No.</p>	The guidance can be found here .	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>119, 1988) (as amended) to assess the privacy impacts of remote working arrangements. The guidance explains that:</p> <ul style="list-style-type: none"> • the Australian Privacy Principles (APPs) continue to apply; • though changes in working practices may have already been made, it is never too late to conduct a PIA, which should also be an iterative process during the life of any project; • organisations should undertake a threshold assessment in the first instance to establish whether a PIA is required; • the scale and scope of a PIA is dependent on the particular project, so if only minor adjustments are required, a PIA need not be very detailed; • a PIA may not be needed if changes to remote working arrangements do not change existing information handling practices and the privacy implications have already been assessed. <p>In addition, the guidance outlines a number of key factors that should be considered when assessing</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			personal information handling in remote working arrangements, raising questions on each. Factors include: governance, culture, training, ICT security, access security, data breaches and physical security.		
Australia	Office of the Australian Information Commissioner (OAIC)	1/4/20	<p>OAIC issues a statement on Covid-19 and protection of personal information</p> <p>The OAIC statement reiterates privacy guidance it developed for public and private organisations, in particular in relation to keeping workplaces safe and properly handling personal information as part of the Covid-19 coronavirus response The guidance includes:</p> <ul style="list-style-type: none"> • "need-to-know" basis for using and disclosing personal information of individuals (including health information); • collecting, using or disclosing the minimum amount of personal information, as reasonably necessary to prevent or manage the pandemic response; • informing employees on how their personal information will be handled in response to any 	The statement is available here .	Data protection-general guidance Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>potential or confirmed Covid-19 case in the workplace;</p> <ul style="list-style-type: none"> implementing appropriate security measures, including where employees are working remotely. 		
Australia	Office of the Australian Information Commissioner (OAIC)	27/3/20	<p>OAIC convenes National Covid-19 Privacy Team and issues statement on the response of Australian regulators to the Covid-19 coronavirus pandemic</p> <p>The OAIC has issued a statement on the response of Australian regulators to the Covid-19 pandemic. The OAIC further announced that it has convened a National Covid-19 Privacy Team comprising the OAIC and states and territories with privacy laws to respond to proposals with national implications.</p> <p>The OAIC acknowledges the need for personal information to be used to address the public health crisis and highlights the mechanisms in state, territory and federal privacy laws to permit the exchange of critical information in these circumstances.</p> <p>The OAIC also stresses the importance of ensuring personal information is handled in a way that is reasonably necessary to prevent and manage Covid-</p>	The press release is available here .	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			19 and that it is protected. The OAIC recognises the need to act fast to deal with the pandemic but reiterates the value in carrying out short-form privacy impact assessments to help ensure personal information is processed in a way that is proportionate, necessary and reasonable.		
Australia	Office of the Australian Information Commissioner (OAIC)	18/3/20	<p>OAIC issues guidance on using and disclosing personal information including regarding remote working</p> <p>The OAIC issued guidance on using and disclosing personal information including information to be provided to staff regarding processing and security in relation to remote working. In particular the OAIC clarified:</p> <ul style="list-style-type: none"> the data protection law allows processing of employee health information under the employee records exemption (which applies where the information about employees is used or disclosed for a purpose directly related to an employment relationship between the employer and individual); employers may inform staff that a colleague or visitor has or may have contracted Covid-19 	<p>Coronavirus (COVID-19): Understanding your privacy obligations to your staff is available here.</p> <p>Guidance on the employee records exemption is available here.</p>	<p>Data protection-general guidance</p> <p>Cybersecurity and information security</p> <p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>but should only use or disclose personal information that is reasonably necessary in order to prevent or manage Covid-19 in the workplace. Whether disclosure is necessary should be informed by advice from the Department of Health;</p> <ul style="list-style-type: none"> agencies and private sector employers can collect health information about individuals without consent to prevent or manage the risk and/or reality of Covid-19 to ensure that necessary precautions can be taken in relation to that individual and any other individuals that may be at risk; the most relevant situation in which it is permitted to use the information for a secondary purpose under the Australian Privacy Principle 6 is "lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety". This applies when: (a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>prevent a serious threat to the life, health or safety of an individual, or to public health or safety.</p> <p>For employees working remotely, similar security measures as those that apply in normal circumstances will need to be considered and organisations should keep up to date with recommendations from the Australian Cyber-security Centre.</p> <p>Amongst other measures they should:</p> <ul style="list-style-type: none"> • increase and test cybersecurity measures; • ensure devices have up-to-date security and are stored safely when not in use; • use work – not personal – email accounts; and • implement multi-factor authentication for remote access. <p>The OAIC notes that government agencies are required to undertake a Privacy Impact Assessment for all high privacy risk projects or initiatives that involve new or changed ways of handling personal information.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Australia	Australian Cyber Security Centre (ACSC)	22/5/20	<p>ACSC publishes guidance for critical infrastructure providers concerning cybersecurity during the Covid-19 coronavirus pandemic</p> <p>The ACSC has published cybersecurity guidance directed at critical infrastructure providers (e.g. power and water providers), particularly addressing remote working practices.</p>	<p>The press release is available here.</p> <p>The guidance is available here.</p>	Cybersecurity and information security
Australia	Australian Cyber Security Centre (ACSC)	8/5/20	<p>ACSC warns of APT actors targeting health sector organisations and Covid-19 coronavirus essential services</p> <p>The ACSC announced that it is aware of advanced persistent threat (APT) actors targeting health sector organisations and research facilities focusing on the response and prevention of the Covid-19 coronavirus pandemic.</p> <p>Specifically, APT actors may focus on those organisations with sensitive personal and medical data or intellectual property relating to the development of solutions such as vaccines, treatments, and research. Phishing, ransomware and brute force attacks are all possibilities. Indeed,</p>	The warning is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Australian health sector entities have been impacted by Coronavirus-related phishing attacks.</p> <p>The ACSC recommended certain cybersecurity mitigations including, amongst other things:</p> <ul style="list-style-type: none"> • multi-factor authentication; • blocking macros; • regular updates; • patching of software; and • email content scanning. <p>The ACSC reminded readers of its ReportCyber web portal for reporting cyber incidents.</p>		
Australia	Australian Cyber Security Centre (ACSC)	7/4/20	<p>ACSC publishes cybersecurity guidance for small businesses during Covid-19 coronavirus outbreak</p> <p>ACSC's published cybersecurity guidance for small businesses in the context of the Covid-19 coronavirus is entitled "COVID-19: Protecting Your Small Business". The guidance aims to assist small businesses to protect themselves against</p>	<p>The guidance is available here.</p> <p>The accompanying press release can be found here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>cyberattacks, highlighting, in particular, the importance of:</p> <ul style="list-style-type: none">• security measures such as:<ul style="list-style-type: none">○ enabling multi-factor authentication;○ backups of data;○ keeping safe strong passwords;○ updating software and operating systems;○ avoiding scam emails (phishing);• measures to be taken in respect of remote working, such as:<ul style="list-style-type: none">○ ensuring portable devices are updated;○ avoiding public Wi-Fi;○ considering physical security;○ training employees on their cybersecurity responsibilities.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Australia	Australian Cyber-security Centre (ACSC)	13/3/20	<p>ACSC issues guidance on good cybersecurity measures to address the cyber threat in preparing for the Covid-19 coronavirus</p> <p>The ACSC recommends incorporating proactive strategies, including:</p> <ul style="list-style-type: none"> • reviewing business continuity plans and procedures; • update and patch systems, including VPNs and firewalls; • scaling up and test in advance of cybersecurity measures in anticipation of the higher demand on remote access technologies; • ensuring that work devices (e.g. laptops and mobile phones) and remote desktop client are secure; • implementing multi-factor authentication for remote access systems and resources, including cloud; • ensuring protection against DoS attacks; 	Guidance is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> informing and educating staff and stakeholders in cybersecurity practices, with specific attention to social engineering; making sure that staff working from home have physical security measures in place. 		
Australia	Australian Digital Health Authority (ADHA)	26/3/20	<p>ADHA gives more apps access to My Health Record and highlights the security and safety requirements applicable to health information</p> <p>The ADHA has announced that it has enabled more mobile apps to connect to My Health Record to give consumers more choice about the ways they get real time access to their health information. ADHA highlighted that Australia needs a connected healthcare system now more than ever and how important it is that the system is accessible, progressive and secure.</p> <p>Over 22 million Australians have a My Health Record, and these records contain over 1.8 billion documents with information relating to hospital visits, pathology test results, medicines, imaging reports and summaries of health status.</p> <p>The ADHA made it clear that the security and safety of people's health information is their priority and the</p>	The press release is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>agency has implemented a range of new requirements that need to be met by connecting apps. These requirements include:</p> <ul style="list-style-type: none"> • mandatory clauses in agreements with app operators preventing them from making a copy of systems data or using it for a secondary purpose; • additional obligations relating to the commercial model, quality processes and company ownership of app providers; and • independent audit obligations for app providers. <p>These restrictions are backed up by civil penalties of up to AU\$1.575 million, per offence, for non-compliance. Criminal penalties may also apply under the My Health Records Act 2012.</p>		
China	Cyberspace Administration of China (CAC)	9/2/20	<p>CAC issues general guidance on processing personal information for epidemic prevention and control</p> <p>The CAC issued a general notice, which clarifies that personal information cannot be collected without the consent of individuals concerned, unless specifically</p>	The notice is available here (only in Chinese).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>authorised by the Health Department of the State Council of the People's Republic of China and subject to requirements of applicable law.</p> <p>The notice further clarifies that the use of Big Data analytics for various aspects of containing the coronavirus epidemic, e.g. prevention and control of virus dissemination in the population, can be performed by private entities under supervision of relevant governmental authorities.</p>		
Hong Kong (SAR), China	Legislative Council Panel on Health Services (Panel)	10/4/20	<p>Panel discusses with the Administration measures for prevention and control of Covid-19 coronavirus</p> <p>The Panel held a special meeting on 8 April 2020 to discuss prevention and control measures taken by the Administration in response to the outbreak of Covid-19 coronavirus. Papers for the meeting were released, including a discussion paper prepared by the Administration, an updated background brief and the Administration's response to a letter from a member of the Panel.</p> <p>The discussion paper offered an update on, amongst others, key measures adopted by the Administration to prevent and control the spread of Covid-19 coronavirus in Hong Kong. It also provided a chronology of major events and measures (as at 6 April 2020), setting out measures taken by the</p>	<p>The discussion paper is available here. The background brief is available here. The Administration's response to the letter from Hon Tanya Chan is available here (only in Chinese).</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Administration to prevent and control Covid-19 coronavirus as the numbers of confirmed cases in Hong Kong and of portable cases increased. Set out below are some of the relevant measures:</p> <ul style="list-style-type: none"> • Enhancing surveillance – extending the health declaration arrangement to all inbound travellers, extending the scope of a laboratory surveillance programme conducted by the Centre for Health Protection to cover all asymptomatic inbound travellers from all places outside China, and extending the scope of an enhanced laboratory surveillance programme conducted by the Hospital Authority to cover outpatients with fever, respiratory symptoms or mild chest infection and to cover around ten viruses apart from Covid-19 coronavirus. • Surveillance of compulsory quarantine – requesting that relevant persons who failed to share their real-time locations with their mobile phones at the boundary control points wear electronic wristbands and asking all inbound travellers arriving at the Hong Kong 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>International Airport to activate the "StayHomeSafe" mobile app.</p> <ul style="list-style-type: none"> • Risk communication – setting up a hotline for contact tracing, launching an Interactive Map Dashboard to provide the latest Covid-19 coronavirus situation and uploading a list of buildings where persons under compulsory quarantine are conducting quarantine onto the relevant government website. <p>The background brief provides, amongst others, a summary of the concerns of members of the Panel on the prevention and control measures taken and of the Administration's responses. Amongst other enquiries, there were enquires from the Panel about the effectiveness of the surveillance of compulsory quarantine. The Administration responded that, amongst others, violation of the compulsory quarantine requirement was a criminal offence and that more manpower had been deployed to detect breach cases with the aid of an electronic monitoring system, conducting spot checks and making telephone calls to persons under compulsory quarantine.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Hong Kong (SAR), China	Office of the Privacy Commissioner for Personal Data (PCPD)	30/3/20	<p>PCPD issues guidance for employers and employees in relation to Covid-19 coronavirus</p> <p>The PCPD issued brief guidance addressing the data privacy issues related to the Covid-19 coronavirus pandemic in the employment context.</p> <p>The Privacy Commissioner for Personal Data Mr Stephen Kai-yi Wong stated that the public health and safety of the community in times of the pandemic remains the primary concern of the PCPD. He further noted that compliance with data protection laws should not be seen as hindering the measures taken to combat the pandemic, in view of the compelling public interests in the current public health emergency. The PCPD pointed out that the data protection laws do not hinder the collection and use of personal data in the public interest and/or in the interest of public health.</p> <p>In relation to employers collecting and processing additional data of their employees to help control the spread of the Covid-19 coronavirus, the PCPD stressed that while there may be a legitimate basis for such processing, it should be specifically related to and used for the purposes of public health and limited in both duration and scope as required in the</p>	The guidance is available here .	Data processing-employment Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>particular situation. Collecting additional data must still adhere to the principles of data minimisation, purpose specification and use limitation. It must be necessary, appropriate and proportionate to the intended purpose.</p> <p>The PCPD further recommended organisations and their employees to be vigilant about cyber threats. The PCPD noted additional risks of remote working arrangements made by many organisations for reducing social contacts, including the risks of using lower-tech home solutions, theft or loss of portable devices, more strain on information technology staff, and cyber criminals taking advantage of the emergency situation by camouflaging password spoofing messages or malware as health alerts.</p>		
Hong Kong (SAR), China	Office of the Privacy Commissioner for Personal Data (PCPD)	26/2/20	<p>PCPD addresses the use of social media data by government to track potential Covid-19 coronavirus carriers</p> <p>The PCPD issued a statement about the use of social media platforms by governmental authorities in order to track potential carriers of coronavirus. The PCPD clarified that although the Personal Data (Privacy) Ordinance (Cap 486) (PDPO) requires that an individual's prior consent is obtained to use their</p>	The statement is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>personal data for a different purpose than originally intended (in this case, for tracking potential carriers of coronavirus), it is subject to exemptions relating to safeguarding the physical or mental health concerns of the data subject or any other individual in the interests of public health.</p> <p>The PCPD discussed in detail applicable international and national law and concluded that under current circumstances, the Government may collect and use information "obtainable offline or online with the aid of devices, applications, software or supercomputers" to track potential Covid-19 coronavirus carriers in the interests of both the individuals concerned and the public.</p>		
<p>Hong Kong (SAR), China</p>	<p>Office of the Privacy Commissioner for Personal Data (PCPD)</p>	<p>21/3/20</p>	<p>PCPD addresses privacy issues arising from Covid-19 coronavirus</p> <p>The PCPD issued a statement about certain issues that arose from the Covid-19 coronavirus pandemic. The PCPD stressed that it was justifiable for organisations, in particular public health authorities, to collect, use, process and retain personal data to protect the community from serious threats to public health.</p>	<p>The statement is available here.</p>	<p>Data protection-general guidance Data processing-employment Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The PCPD pointed out that personal data could be used for protecting public health without having to obtain the consent of the data subject and that medical practitioners could disclose personal data to the public health authorities in order to comply with the relevant public health legislation.</p> <p>For employers who needed to collect health data of their employees to protect the latter and the wider community, the PCPD recommended them to use a self-reporting system and to provide employees with a personal information collection statement when or before their data were collected.</p> <p>The PCPD further clarified that while data protection laws should not hinder measures taken to combat Covid-19 coronavirus, organisations should not derogate their responsibilities in handling personal data throughout the entire life cycle of the data, including data collection and data retention.</p> <p>The PCPD stressed that anti-virus measures that might encroach on the privacy right of the individuals concerned shall be proportionate to achieving the purpose of combating the pandemic.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Hong Kong (SAR), China	Office of the Privacy Commissioner for Personal Data (PCPD)	12/2/20	<p>PCPD addresses the use of video calls by government to ensure compliance with quarantine requirement</p> <p>The PCPD issued a statement about the use of video calls by government authorities to ensure compliance by persons under mandatory quarantine with the requirement to remain at the locations specified in the quarantine order.</p> <p>The PCPD noted that while the location data might involve places of residence where a high degree of privacy was expected, government authorities collected such data for a lawful purpose of effective implementation of the quarantine measures and the data collected were not excessive. The PCPD also noted that consent from the persons under quarantine had been obtained in accordance with the law.</p> <p>The PCPD clarified that data users might disclose personal data relating to the health of the data subject to a third party without the consent of the data subject if restrictions on disclosure would otherwise be likely to cause serious harm to the health of any individuals.</p>	The statement is available here .	Data processing- public authorities
India	Data Security Council of India (DSCI)	24/4/20	<p>DSCI publishes a DSCI Privacy Outlook Advisory, considering data protection during the Covid-19 coronavirus pandemic</p> <p>The Privacy Outlook, in the form of a DSCI Advisory (the Advisory) highlights the privacy implications of</p>	The Advisory is available here .	Data processing- public authorities Data processing- employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the Covid-19 coronavirus for various stakeholders and advises on privacy and data protection practices.</p> <p>The Advisory addresses healthcare privacy conditions, noting the importance of:</p> <ul style="list-style-type: none"> • notifying patients of all information and personal data collected; • having specific protocols in place for collecting data to ensure consent of the patient at every stage; • limiting use of information collection from the patient to the purposes notified to the patient; • allowing the patient an option of refusal to provide any information not required for treatment; • disclosing medical records only with prior patient approval; and • implementing internal and external audit mechanisms. <p>The Advisory notes that, whilst collecting data to help contain and track the Covid-19 coronavirus, government authorities must be mindful of data</p>		Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>protection principles, in particular collection and use limitation to ensure collection of personal data is necessary and proportionate. The Advisory goes on to specify that:</p> <ul style="list-style-type: none"> • the majority personal data usage should be made once aggregated to non-identifiable data; • transparency with the public about personal and aggregated anonymised data use should be maintained and usage of data lawful and fair; • the purpose for which personal and anonymised data is being shared should be clearly described and only used for that purpose; • rules prohibiting re-identification of aggregated non-identifiable data should be enforced except as permitted by law and notified to identified individuals; • data privacy impact assessments should be conducted in respect of any aggregated non-identifiable data received; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • data collected from individuals should be deleted when no longer needed/after a fixed period; • evidence should be provided that they have acted in accordance with assurances provided and establish an independent oversight board to monitor adherence to these principles. <p>The Advisory also provides recommendations for remote working, both for employees and employers, noting the importance of reassessing data protection strategies, data management practices, and remaining compliant with regulatory requirements. It recommends conducting data protection impact assessments and undertaking training and awareness raising activities in respect of privacy.</p>		
India	Data Security Council of India (DSCI)	22/4/20	<p>DSCI publishes guidance for cybersecurity in specific industries in light of Covid-19 coronavirus pandemic and cyberattack warning</p> <p>The DSCI has issued guidance, as a DSCI Advisory (the Cyberattack Advisory), and published a technical report regarding the increase in cyberattacks during the Covid-19 coronavirus pandemic. The DSCI notes that the cyberattacks vary</p>	<p>The Cyberattack Advisory is available here and the technical report is available here.</p> <p>The portal for the DSCI Advisories is available here. The</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>in nature but that the Maze ransomware attack is particularly prevalent.</p> <p>The DSCI has published a technical report setting out information including the modus operandi of Maze, the IP addresses it uses and how it affects desktop appearance. The report also provides specific recommendations to help organisations avoid a Maze ransomware attack, including installing ad blockers and implementing strong email security software. Further recommendations are included in the accompanying Cyberattack Advisory, such as ensuring that the environment does not run unsigned macros, conducting phishing awareness campaigns, locking down RDP, deploying backup strategies, segmentation of networks and encouraging the implementation of best practices for granting system permissions to files, patching, configuring systems, amongst others.</p> <p>The DSCI's publications on Maze ransomware follow its issuance of four DSCI Advisories for specific industries and groups including in response to increased cybersecurity risk due to the Covid-19</p>	<p>Advisories themselves are available here (employees), here (healthcare industry) and here (law enforcement).</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>coronavirus pandemic. Specifically, the DSCI has issued the following guidance in its Advisories:</p> <ul style="list-style-type: none"> • on 18 March, an Advisory on security measures when working from home, see further in this overview; • on 2 April, an Advisory on working from home for employees generally. This includes guidance on general productivity at home and the security of home networks, software, assets, portable media, passwords, emails and internet use. It also promotes awareness of different types of scams and cyberattacks, including donation scams, phishing, and social engineering; • on 9 April, an Advisory for hospitals and the healthcare industry. This identifies the medical industry as a particular focus of cyberattacks due to its round-the-clock and crucial work at this time. The guidance sets out the specific types of scam to which the medical industry is particularly vulnerable, such as theft of patient data and sale of falsified medical equipment. The Advisory contains specific 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>recommendations for the medical industry to prevent such scams and attacks in a three-tier format: at staff level, at IT infrastructure level and at back-up level; and</p> <ul style="list-style-type: none"> on 11 April, an Advisory for law enforcement agencies. This includes guidance for police officers on protecting themselves from exposure, police station hygiene, dealing with Covid-19 coronavirus positive suspects and when taking in digital assets, and management advice for police leadership. The Advisory also contains cyber security best practice information and recommendations for dealing with common cybercrime scenarios. 		
India	Ministry of Housing and Urban Affairs (MHUA)	21/4/20	<p>MHUA announces launch of Coronavirus tracking app</p> <p>The Salyam mobile app was launched by the Pune Municipal Corporation to track quarantined citizens during the Covid-19 coronavirus pandemic as part of the National Smart Cities Mission (the Salyam App). The Salyam App is separate to the app launched by MEITY on 2 April 20 (see further in this overview) and aims to monitor people who have recently returned from international travel and those discharged</p>	The press release is available here .	<p>Mobile apps and new technology</p> <p>Data processing – location data</p> <p>Data processing – public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			following Covid-19 coronavirus treatment. Teams of people will follow up with such individuals regarding their health status and access to support. They will also check if those under home quarantine have downloaded the app. GPS tracking (which individuals are advised to keep on) will provide alerts to the City Administrator if such individuals leave their home and a local ward or the local police will visit the family. The degree of departure from the home will be colour coded.		
India	Department of Science and Technology of the Government of India (DST)	15/4/20	<p>DST publishes press release announcing platform on geospatial information for tracking spread of Covid-19 coronavirus</p> <p>The DST has announced its launch of an Integrated Geospatial Platform that will use geospatial information tracking individuals infected with the Covid-19 coronavirus. The data used relates to India only and the DST aims to use this tool to help decision-making during the pandemic.</p> <p>The press release confirms that the platform will complement the Aarogya Setu tracking app launched by the Indian government.</p>	The press release is available here .	<p>Mobile apps and new technology</p> <p>Data processing-location data</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The DST also states that authorities in several regions of India have provided geospatial data services for integration with the relevant health data sets for the purpose of combating the pandemic.</p> <p>The press release notes that mobile application SAHYOG, as well as the web portal (https://indiamaps.gov.in/soiapp/) has been customised to collect Covid-19 coronavirus specific geospatial datasets through community engagement to augment the response activities by Government of India to the pandemic.</p> <p>The initial intention of the integrated platform is to help strengthen the public health delivery system and thereafter to provide support to citizens and agencies dealing with wide ranging challenges created by the pandemic "through the seamless provision of spatial data, information, and linkage between human, medical, technological, infrastructural and natural resources".</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
India	Ministry of Electronics and Information Technology (MEITY)	2/4/20	<p>MEITY announces the launch of Covid-19 tracking app</p> <p>The Aarogya Setu App (the App), has been developed in public-private partnership, to track the Covid-19 coronavirus infection. The MEITY noted that the App will enable people to assess infection risks of the virus, and will calculate this based on their interaction with others, using Bluetooth technology, algorithms and artificial intelligence.</p> <p>In addition, once installed on a smart phone, the App will detect other devices which contain the app that come into proximity of that phone, and will calculate risks based on contacts tested positive.</p> <p>The MEITY also notes that personal data collected by the App will be encrypted, and will remain secure on the phone until required to facilitate medical intervention.</p>	<p>The press release of MEITY is available here.</p> <p>The press release on the government portal is available here.</p>	Mobile apps and new technology
India	Ministry of Health and Family Welfare (MOHFW)	25/3/20	<p>MOHFW issues guidelines on telemedicine practices</p> <p>India's MOHFW has issued detailed guidelines to assist registered medical practitioners (RMPs) in providing healthcare services remotely. The Telemedicine Practice Guidelines include the</p>	The guidelines are available here .	Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>guidelines for technology platforms enabling telemedicine.</p> <p>The guidelines state that RMPs must comply with data protection and privacy laws to protect patient privacy and confidentiality but they will not be held liable for a breach of the patient's privacy and confidentiality if there are reasonable grounds to believe the patient's confidentiality has been compromised due to a technology breach or by a person other than the RMP.</p> <p>The guidelines also describe how RMPs should identify patients and obtain their implied or express consent, what methods of communication can be used and how to manage situations where the RMP is communicating with a caregiver rather than the patient. A section of the Guidelines is dedicated to maintaining a digital trail and data retention.</p>		
India	Data Security Council of India (DSCI)	18/3/20	<p>DSCI publishes recommendations on security measures for working from home</p> <p>The DSCI has published an recommendations in an Advisory document on working from home. The advisory document outlines requirements to secure</p>	<p>The press release is available here.</p> <p>The Advisory document is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>companies' networks whilst allowing remote access for employees.</p> <p>The guidance states that a secure connection to the workplace, utilising virtual desktop applications and only using VPNs through company-owned hardware, is important to achieve this aim. Remote access should be monitored, controlled and encrypted, networking segregated or limited where possible and unnecessary ports and applications closed/removed.</p> <p>The document also advises companies to provide live 24/7 IT support and ensure staff follow basic security practices and procedures, which include:</p> <ul style="list-style-type: none"> • strong password policies; • firewalls; • awareness of increased phishing attack threats; and <p>protection of confidential information when working from home.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Japan	National Centre of Incident Readiness and Strategy for Cybersecurity (NISC)	14/4/20	<p>NISC publishes guidelines on teleworking security in light of Covid-19 coronavirus pandemic</p> <p>The NISC has published a guidance document setting out various security considerations relating to the performance of telework as a result of the Covid-19 coronavirus pandemic. The guidance notes that utilisation of teleworking is rapidly increasing and emphasises its aims to both increase awareness and inform the general public of the basics.</p> <p>The document provides guidance on the precautions to be taken for teleworking in a government agency context and for important infrastructure operators. The NISC emphasises that it is important for such agencies to understand the security risks of teleworking and manage these appropriately.</p> <p>The NISC's advice includes recommendations on preparing staff for starting telework, setting up and improving the VPN, using encryption techniques, confirming how to report an incident and processes. In particular, it highlights security risks with remote conference systems and references the Zoom app in particular, recommending that the potential risks are investigated. The NISC also sets out specific security</p>	The guidelines are available here (only in Japanese).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>standards that government agencies are expected to meet.</p> <p>The guidance further sets out practical recommendations for teleworking employees, which includes amongst others, not sharing telework photos that contain confidential information on social media, avoiding the leak of information in the background of videoconferences, using complex passwords and multi-factor authentication, being mindful of theft or loss of devices, taking care to avoid phishing emails, and not discussing work in public places.</p>		
Japan	Personal Information Protection Commission (PPC)	2/4/20	<p>PPC issues guidance on processing personal data in preventing the transmission of the Covid-19 coronavirus</p> <p>The PPC issued brief guidance on the processing of personal data during the Covid-19 coronavirus pandemic in the form of FAQs for employers and guidance on the relevant provisions of the Act on the Protection of Personal Information (the Act).</p> <p>The guidance notes that a "personal information handling business operator" (or PIHBO) may process personal data in accordance with the Act for purposes other than the original purpose, and disclose personal</p>	<p>The guidance is available here and the FAQs are available here (in Japanese).</p> <p>The guidance and the FAQs are available here (in English).</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>data to a third party without consent in certain situations, including:</p> <ul style="list-style-type: none"> • where a central government body requests the data in relation to processing activities permitted by law and where the PIHBO's lack of cooperation or obtaining the data subject's consent would interfere with the performance of such activities (the PPC refers to Article 16(3)(iv) and Article 23(1)(iv) of the Act); and • where necessary to protect human life and safeguarding public health (the PPC refers to Article 23(1)(ii) and (iii) of the Act). <p>The FAQs note that, where an employee has contracted the Covid-19 coronavirus, employers do not need to obtain the employee's consent to notify other employees or third parties that they may have come in contact with the employee.</p>		
<p>New Zealand [Updated as at 28 May 2020]</p>	<p>Privacy Commissioner of New Zealand (OPC)</p>	<p>27/5/20</p>	<p>OPC releases assessment of contact tracing solutions and statement regarding collection of information by retail and the hospitality industry.</p> <p>The OPC has provided a table of information regarding a range of contact tracing apps, including</p>	<p>The assessment is available here. The press release is available here.</p>	<p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>amongst others: NZ Covid Tracker, Rippl, tracing.co.nz.</p> <p>The assessment covers target users, how each solution works, information collected, rights of access, storage of data, retention periods, transparency of the Appius for contact tracing.</p> <p>The OPC also published a press release advising hospitality and retail businesses not to collect too much personal data, for example, when using contact tracing tools.</p>		
New Zealand	Privacy Commissioner of New Zealand (OPC) New Zealand Ministry of Health	20/5/20	<p>OPC issues a statement welcoming the New Zealand Ministry of Health’s “Covid Tracer” app</p> <p>The OPC has welcomed the Ministry of Health’s Covid-19 coronavirus contact tracing app, the Contact Tracer, noting OPC involvement in development, the use of privacy by design and the conduct of a privacy impact assessment.</p> <p>The OPC confirmed that the information collected by the app will be held for public health purposes only and will not be further shared with other agencies unless required for contact tracing purposes.</p>	<p>The press release is available here.</p> <p>The PIA is available here.</p> <p>The Ministry of Health launch information, explanations and FAQs are available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Ministry of Health’s launch information provides detail on how the app works, sets out key FAQs and addresses privacy issues such as:</p> <ul style="list-style-type: none"> • recipient of personal contact details and information shared through the app (National Close Contact Service) • use of multifactor authentication; • reliance on Amazon web services; • ability to uninstall app and delete data from device (though not from the “digital diary”). 		
New Zealand	Privacy Commissioner of New Zealand (OPC)	20/5/20	<p>OPC publishes a statement explaining the powers under the new Public Health Act and how they relate to the use of contact tracing apps</p> <p>The OPC has issued a statement addressing the legal basis for collecting, using and sharing personal data in the context of the Covid-19 coronavirus noting in particular that the emergency powers established by the Civil Defence National Emergencies (Information Sharing) Code 2013 will soon will come to an end on 11 June 2020.</p> <p>The Code provides authority for agencies to collect, use or disclose personal information during a state of</p>	<p>The statement is available here.</p> <p>The explanatory blogs of 29 April 2020 and 26 March are available here and here.</p>	<p>Data protection-general guidance</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>national emergency for purposes directly related to the Government's response to this emergency (in this case, the Covid-19 coronavirus pandemic) where the relevant agency reasonably believe all of the following criteria are met:</p> <ul style="list-style-type: none"> • the individual concerned may be involved in the national emergency – it was considered that this related to all New Zealanders; • the collection, use or disclosure is for a purpose that directly relates to the government or local government management of response to, and recovery from, the state of national emergency; and • personal information is disclosed to one of the following agencies: <ul style="list-style-type: none"> ○ a public sector agency; ○ an agency that is, or is likely to be, involved in managing or assisting in the management of the emergency; or ○ an agency directly involved in providing repatriation, health, financial or other 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>humanitarian assistance services to individuals involved in the emergency.</p> <p>The Code operates as an extension to the existing New Zealand Health Information Privacy Code exception (permitting disclosure of information in the context of a “serious threat to public health or safety”), so there remains a legal basis for the use, collection and sharing of personal information in any case. However, the new Public Health Act 2020 (specifically section 11) also grants a power to require information, justified if urgently needed to prevent or contain the Covid-19 coronavirus pandemic. Any such order must also be presented to Parliament as soon as practicable and typically remains in place for a month (unless revoked or extended).</p>		
New Zealand	Privacy Commissioner of New Zealand (OPC)	7/4/20	<p>Privacy Commissioner releases blog post on data protection matters and regional disclosure of Covid-19 coronavirus cases</p> <p>The OPC has published a blog post setting out its response to criticism received by the District Health Board in Waikato, New Zealand, for not disclosing the number of Covid-19 coronavirus cases in each of the region's districts, citing privacy concerns.</p>	The blog post is available here .	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The OPC emphasises that while a cautious approach is well received, the New Zealand Privacy Act applies only to information about an identifiable individual. Health information, such as Covid-19 coronavirus status, should be available to everyone who needs it but on a basis of only as much as they need, and not any more.</p> <p>The blog post urges local health boards to take a proportionate approach to releasing Covid-19 statistics, disclosing only what is necessary for the public health response to the virus. It acknowledges that privacy concerns may arise if case numbers are publicly reported for a very small town, for example. The right to privacy around health information remains, although somewhat qualified by the need to control the spread of the virus, but there is no value in the distribution of health information about others to those who have no use for it.</p>		
New Zealand	Privacy Commissioner of New Zealand (OPC)	3/4/20	<p>Privacy Commissioner issues statement on police tracing system used to trace travellers in relation to the Covid-19 coronavirus</p> <p>The OPC issued a statement confirming it had received a briefing from the New Zealand police in relation to the software and website used to contact,</p>	The statement is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>register and trace individuals returning to New Zealand following international travel.</p> <p>The statement noted concerns in relation to the appearance and authenticity of text messages sent by police to individuals returning to New Zealand and the website used by individuals to opt-in to the tracing scheme. The OPC confirmed that the website is being redeveloped to ensure its official function is clear.</p> <p>The statement confirms that the police are undertaking a privacy impact assessment and security review of the tracing website and software, which had been repurposed from a previous search and rescue function and scaled up for the Covid-19 emergency. The OPC confirmed that it considers the police took appropriate steps to ensure the system is proportionate.</p>		
New Zealand	Privacy Commissioner of New Zealand (OPC)	30/3/20	<p>Privacy Commissioner issues data protection guidance for employers in the healthcare sector</p> <p>The OPC published a blog post setting out specific guidance for general practitioners and other frontline health professionals on their privacy obligations in the workplace arising out of the Covid-19 coronavirus.</p>	The blog post is available here .	<p>Data processing-public authorities</p> <p>Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The blog post confirms that employers in the healthcare sector must adhere to the New Zealand Privacy Act, which permits employers to collect information about their employees' health status if it is needed for a lawful purpose such as health and safety, providing that information regarding how that information will be handled has been given to the employee.</p> <p>The OPC explains that employers should handle the situation alongside any employee who fears they may have a communicable disease, such as by undertaking to keep the information confidential and assuring the employee that they will not be disadvantaged as a result, but accepts that in a small practice this may not be practical.</p> <p>The blog post also sets out the circumstances under which disclosure of health data is permitted, such as where there is reason to believe the use or disclosure is necessary in order to prevent or lessen the risk of a serious threat to someone's safety, wellbeing or health. The OPC believes that the risk of transmission of Covid-19 coronavirus is likely to be considered such a "serious threat". The blog post also confirms that it is at the discretion of the workplace whether to</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			tell other employees that a colleague is off sick, in line with any policies in place.		
New Zealand	Privacy Commissioner of New Zealand (OPC)	26/3/20	<p>OPC publishes blog post providing guidance on data subject access rights during Covid-19 coronavirus pandemic</p> <p>The OPC released a blog post setting out guidance for entities and individuals about personal information access requests by individuals during the Covid-19 coronavirus emergency.</p> <p>The OPC clarified that agencies closed for business due to the lockdown might not be able to provide information within the statutory term of 20 working days. The OPC recommended that individuals who need the information before a specific date should indicate this in their access requests but be also understanding about possible delays due to the strain from the Covid-19 coronavirus measures.</p> <p>Nevertheless, the 20-day deadline period still applies and agencies should look for one of the permitted reasons or seek an extension and timely notify the individual about the expected delay.</p>	The blog post is available here .	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			If information is not readily retrievable due to the lockdown, this will be a basis to refuse the request and address it once the lockdown has been lifted.		
New Zealand	Privacy Commissioner of New Zealand (OPC)	25/3/20	<p>OPC clarifies the effects of the national emergency under the Civil Defence Emergencies Act on privacy rights</p> <p>The OPC clarifies that a state of national emergency (as declared in the case of the Covid-19 coronavirus) triggers the operation of the Civil Defence National Emergencies (Information Sharing) Code 2013 under the Privacy Act 1993.</p> <p>The Code means, for example, that public and private entities can now process personal information in order to manage or respond to the Covid-19 coronavirus. For instance, employers can now disclose required employee information to the Ministry of Social Development to access the government wage subsidy without obtaining prior employee authorisation. The OPC recommends still notifying individuals about the use of their information if this is reasonably practicable.</p> <p>The Code provides authority for agencies to collect, use or disclose personal information for purposes</p>	The guidance is available here .	Data protection-general guidance Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>directly related to this emergency, if certain criteria are met:</p> <ul style="list-style-type: none"> • the individual concerned is involved in the national emergency (noting it currently covers anyone in New Zealand); • processing is limited to a purpose that directly relates to the management of, response to and recovery from the state of national emergency caused by the Covid-19 coronavirus pandemic; and • in the case of a disclosure, the personal information is disclosed to a public sector agency, an agency involved in managing or assisting in the management of the emergency, or an agency directly involved in providing repatriation, health, financial or other humanitarian assistance services to individuals involved in the emergency. <p>As such, agencies can use the Civil Defence Code, rather than an individual's authorisation, as legal authority to collect, use or disclose that individual's personal information in relation to Covid-19 coronavirus, subject to the limits above.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
New Zealand	Privacy Commissioner of New Zealand (OPC)	13/3/20	<p>OPC issues FAQs on privacy and the Covid-19 coronavirus</p> <p>The OPC released FAQs on the Covid-19 coronavirus to help organisations navigate privacy considerations in situations where there is a risk of exposure to the Covid-19 coronavirus. The guidance highlights the following:</p> <ul style="list-style-type: none"> • under the Health Act 1956, a statutory medical officer designated by the Director-General of Health can oblige event organisers to disclose information about individuals who pose a public health risk; • an exception in the Privacy Act 1993 that permits the use or disclosure of personal information to a medical officer where this is necessary to prevent or lessen a serious threat to public health or security; • if employees return from overseas with possible Covid-19 coronavirus symptoms and self-isolate themselves, there is no health and safety necessity for the employer to disclose this information to other staff members; 	<p>The FAQs are available here.</p> <p>Further collation of FAQs is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> if an employee displays possible Covid-19 coronavirus symptoms at work and is sent home, other employees can be informed about the possible exposure, but by avoiding identifying the employee in question (unless required or unavoidable, such as in small organisation units, or where disclosure is necessary to prevent or lessen the risk of a serious threat to safety, wellbeing or health). <p>The OPC generally recommends taking a common sense approach to disclosing personal information in relation to the Covid-19 coronavirus, noting that in most circumstances, disclosure of the exact reason why an employee is out of the office is not likely to be needed in a workplace.</p> <p>The FAQs relating to the pandemic continue to be expanded, covering, amongst other things, FAQs concerned with:</p> <ul style="list-style-type: none"> access of the individual to information held by another entity; hospitality and events industry and nature of information companies can collect for contact tracing; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • sharing of information between health care providers; and • employee/employer relationship, monitoring and contact tracing information permitted. 		
New Zealand	National Computer Emergency Response Team (CERTNZ)	25/5/20	<p>CERTNZ releases cybersecurity guidance on measures for working from home</p> <p>CERTNZ has published guidance on cybersecurity issues when working from home including, amongst other things:</p> <ul style="list-style-type: none"> • use remote access software; • create strong passwords; • enable two-factor authentication; • ensure that work devices are encrypted, patched and configured appropriately; • address physical security and ensure communication routes are established for reporting devices lost; • ensure end-to-end encryption of communications; and 	<p>The guidance is available here.</p> <p>The associated quick reference guide is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> record all remote working decisions/requirements in a policy. <p>An associated quick guide has also been produced for ease.</p>		
Philippines	National Privacy Commission (NPC)	20/4/20	<p>NPC issues guidance on design and use of new technologies in response to Covid-19 coronavirus pandemic</p> <p>The NPC issued guidance on the design and use of technologies developed in response to the Covid-19 coronavirus pandemic (NPC PHE Bulletin No. 8). The guidance confirms that the NPC, in principle, supports the development and use of such technologies if such technologies protect individual privacy and contain appropriate security measures to protect personal data.</p> <p>The NPC notes that designers of new technologies must ensure that the technology has a legitimate purpose (limited to and consistent with defeating the Covid-19 coronavirus), any data processing is proportionate and ceases when no longer required (with data deleted/disposed of), users of the technologies are informed of the processing activities (and their associated rights, such as via a privacy</p>	The guidance is available here.	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			notice) and appropriate security measures are implemented.		
Philippines	Department of Health (DoH)	14/4/20	<p>DoH launches infection tracing application to monitor Covid-19 coronavirus pandemic</p> <p>The DoH announced the launch of a tracker to enable the public to track the spread of, and the ability of local authorities to respond to, the Covid-19 coronavirus. The tracker provides information in relation to available health facilities, national testing activities, and DoH laboratory testing capabilities, including information based on that collected through the DoH DataCollect application (which gathers daily data from hospitals and other stakeholders on status of health care capacity for example).</p>	<p>The press release is available here.</p> <p>The tracker is available here.</p>	Mobile apps and new technology
Philippines	National Privacy Commission (NPC)	26/3/20	<p>NPC issues bulletin on data protection and Covid-19 coronavirus pandemic</p> <p>The NPC has issued a Filipino-version of its previous guidance released on 19 March 2020 (see the entry below). The guidance reiterates the importance of organisations collecting only personal data that are necessary for the purpose of processing and only disclosing personal data to authorised recipients.</p>	The bulletin, incorporating the guidance issued on 19 March 2020, is available here (in Filipino only).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Philippines	National Privacy Commission (NPC)	19/3/20	<p>NPC issues guidance and FAQs on data protection and Covid-19 coronavirus pandemic</p> <p>The NPC issued guidance and FAQs on the collection, processing and disclosure of personal data during the public health emergency. The guidance is intended to support the government and health practitioners in responding to the Covid-19 coronavirus pandemic. It confirms the importance of only collecting necessary personal data and only disclosing personal data to authorised recipients.</p> <p>The FAQs address a number of scenarios and issues, including:</p> <ul style="list-style-type: none"> • collection of personal information from visitors to workplaces; • completion of questionnaires by employees in relation to travel and medical history; • disclosure of employee personal data by employers to third parties; and • company press releases or statements in relation to suspected or confirmed cases of employees with the Covid-19 coronavirus. 	The guidance and FAQs are available here .	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The NPC highlights that the Department of Health (DoH) is leading the national response to the Covid-19 coronavirus pandemic and, where an employer is required to collect specific data from employees, the employer should follow the DoH's guidance and authority as to what specific data are required and what methods are permitted.		
Singapore	Singaporean Personal Data Protection Commission (PDPC)	16/3/20	<p>PDPC publishes FAQs on collecting visitors data</p> <p>The PDPC published FAQs on the Covid-19 coronavirus, which confirmed that organisations collecting personal data need to comply with the Personal Data Protection Act (PDPA). The FAQs emphasised that pursuant to Schedule 2, 3 and 4 of the PDPA, the collection, use and disclosure of personal data by organisations without consent is only permitted where it is considered necessary in response to an emergency that threatens the life, health or safety of other individuals.</p> <p>The PDPC confirms that it considers the Covid-19 coronavirus outbreak as an emergency that permits organisations to collect personal data of visitors to premises where it is necessary for purposes of contact tracing and other outbreak-related response measures. Organisations may collect visitors NRIC,</p>	The FAQs are available here .	Data processing- employment Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			FIN or passport numbers where necessary to identify individuals in the event of a Covid-19 coronavirus case.		
South Korea	South Korea's Communications Commission (KCC)	11/2/20	<p>KCC issues a statement regarding leaks of personal information relating to the Covid-19 coronavirus online</p> <p>The KCC addressed its concerns about leaks of documents containing personal information of Covid-19 coronavirus patients online and reiterated that disclosure of personal information of patients, other than by the quarantine authority, is illegal and may be subject to civil and criminal penalties.</p>	The statement is available here (only in Korean).	Data protection-general guidance
EUROPE					
EU	European Parliament [Updated as at 21 May 2020]	14/5/20	<p>The European Parliament publishes a statement on privacy and data protection safeguards that must be present Covid-19 coronavirus tracing app.</p> <p>In a plenary debate, the European Parliament highlighted that contact tracing apps must be:</p> <ul style="list-style-type: none"> • truly voluntary; • non-discriminatory; 	The press release is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> transparent; and data collected must be deleted as soon as possible. <p>In addition, MEPs considered that there is a need to retain trust in apps and Commissioner Didier Reynders confirmed that national authorities will work together in relation to Covid-19 coronavirus apps and their interoperability.</p>		
EU	European Parliament	20/4/20	<p>European Parliament announces a European Parliamentary Research Service briefing on mobile devices tracking in connection with the Covid-19 coronavirus pandemic</p> <p>The European Parliament announced that the European Parliamentary Research Service has produced a briefing discussing, amongst other things, mobile device tracking in connection with the Covid-19 coronavirus pandemic.</p> <p>The briefing considers that governments may be justified in limiting certain rights and freedoms in order effectively to tackle the crisis, but these are exceptional and temporary measures and must still comply with applicable laws.</p>	<p>The press release is available here.</p> <p>The briefing is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The briefing discusses use of technology in the fight against the crisis including the use of aggregate data by organisations to map population movements. It also covers individual location-tracking measures using, amongst other things, mobile devices, contact tracing applications, references certain applicable laws, and highlights the approach of Member States and guidance issued by European bodies.		
EU	European Parliament	17/4/20	<p>EU Parliament adopts a resolution on EU Coordinated Action to Combat the COVID-19 Pandemic and its consequences</p> <p>The European Parliament adopted a Resolution on EU Coordinated Action to Combat the COVID-19 Pandemic and its Consequences (the Resolution).</p> <p>The Resolution expresses the EU Parliament's concern regarding the crisis in general and calls on Member States to act in a cooperative way (which it considers has yet to be achieved). It makes a number of more specific calls on a broad range of topics but more particularly regarding data protection, the Resolution:</p> <ul style="list-style-type: none"> calls on the European Commission to develop its capacity for cloud services, while complying 	The Resolution is available here .	Data protection-general guidance Mobile apps and new technology Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>with the ePrivacy Directive and GDPR, to facilitate the exchange at EU level of research and health data by entities working on the development of treatment and/or vaccines;</p> <ul style="list-style-type: none"> • takes note of the European Commission's plan to call on telecoms providers to disclose anonymised and aggregated data in order to limit the spread of Covid-19 coronavirus and the use of national tracking programmes and the introduction of apps allowing authorities to monitor movements, contacts and health data; • addresses the rising use of contact-tracing apps during the crisis, the European Commission's recommendation to develop a common EU approach for the use of such apps and the need for these apps (whether developed at a national or EU level) to: <ul style="list-style-type: none"> ○ be voluntary; ○ use decentralised, rather than centralised databases; ○ account for of the principles of data protection by design; ○ apply data minimisation requirements; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ only process mobile location data in accordance with the ePrivacy Directive and GDPR; • requires full transparency from the European Commission and Member States regarding the functioning of contact-tracing apps, to allow verification of the underlying protocol for security and privacy and checking of the code itself to see whether the application functions as the authorities are claiming; • specifies the need for full transparency on (non-EU) commercial interests of app developers and for clear projections be demonstrated as regards to the positive impact of the apps; • calls on the Commission and the Member States to publish the details of these schemes to allow scrutiny and full oversight by DPAs; and • stresses that national and EU authorities must fully comply with data protection and privacy legislation, and national DPA oversight and guidance. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	European Parliament	1/4/20	<p>The European Parliament has published recommendations on how to protect yourself from cybercrime in the context of the Covid-19 coronavirus</p> <p>The European Parliament notes that increased time online and homeworking can lead to unsafe online practices and opportunities for cybercriminals to exploit weaknesses.</p> <p>It highlights particular risks of the phishing, installing malware and other malicious practices to steal data and access devices. The most common cyberattacks related to Covid-19 coronavirus include:</p> <ul style="list-style-type: none"> • fake messages or links exploiting concerns, driving to malicious websites or including malware themselves, news about miracle cures, fake maps about the spread of the virus, donation requests, emails impersonating healthcare organisations; • fake messages or calls purporting to be from well-known online service providers. trying to get hold of your login and password by offering "help" or threatening the suspension of your account; 	The recommendations are available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • fake messages about non-existent package deliveries. <p>Whilst the European Parliament acknowledges that the EU is working with telecom operators to protect networks against cyberattacks, it flags some particular tips to consider at a personal level. For example:</p> <ul style="list-style-type: none"> • being cautious with unsolicited emails, text messages and phone calls, particularly if they use the Covid-19 coronavirus to pressure you into bypassing the usual security procedures; • securing your home network by, for example, changing the default password for your Wi-Fi network to a strong one, limiting the number of devices connected to your Wi-Fi network and only allowing trusted devices to connect; • strengthening your passwords; • protecting equipment, using, for example, up to date antivirus software; • preventing family and friends from using work devices (so as to avoid accidental data loss or infection). 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	European Commission [Updated as at 21 May 2020]	13/5/20	<p>European Commission announces adoption by eHealth Network of Interoperability guidelines and produces an associated Q&A</p> <p>The European Commission confirms that the Member States' eHealth Network has developed, with its support, and subsequently adopted Interoperability guidelines regarding Covid-19 coronavirus contact tracing apps to build on the Toolbox further described in this overview. The Interoperability guidelines, amongst other things:</p> <ul style="list-style-type: none"> • reiterate the need for apps to be voluntary, transparent, temporary, cybersecure, using pseudonymised data, rely on Bluetooth technology, and be approved by national healthcare authorities; • confirm that national authorities are accountable for their apps and servers, and have flexibility in implementation of those apps; • emphasise the need for tracing apps to communicate with each other such that citizens can use one app to report a positive 	<p>The press release and infographic is available here.</p> <p>The guidelines are available here.</p> <p>The Q&A is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Covid-19 coronavirus test or to receive an alert;</p> <ul style="list-style-type: none"> • highlight that relaxation of freedom of movement measures across the EU depends on interoperability; • caution that the guidelines are a living document, to be used as a baseline by developers; • set out specific minimum requirements for interoperability of contact tracing apps including: <ul style="list-style-type: none"> ○ different protocols determining proximity and exposure risk should not lead to a difference in contact tracing in cross-border scenarios; ○ Bluetooth should be interoperable and include privacy-preserving identifiers; ○ following positive testing the relevant authority should provide an interoperable mechanism to enable a user to confirm infection to the app and a trusted a secure mechanism is 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>required to enable sharing of test results between national health authorities;</p> <ul style="list-style-type: none"> ○ contact with the user should be in their own language, cover measures relevant to location and enable them to seek assistance in their home country; ○ roaming users should be informed of how to contact local health authorities and once such users upload proximity data to home country system, other Member States should be informed of infection risk; ○ mechanisms should be transparent with communication between Member States to enable development and account for changes. <ul style="list-style-type: none"> ● note that technical details are to follow with discussion and resources available to assist Member States and app developers. <p>The guidelines are complemented by a Q&A which covers what and why contact tracing apps are required; how they work; what and why the</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			interoperability guidelines are required; what data (including personal data) is shared between Member States; the need for internet connection (or otherwise) and how to address those without smartphones.		
EU	European Commission	16/4/20	<p>European Commission issues a Toolbox for Covid-19 coronavirus contact tracing and warning apps to establish common approach to technical specifications, interoperability, data protection and cybersecurity</p> <p>The European Commission published a document setting out common approach to the development, use and monitoring performance of mobile apps for tracing and warning about the Covid-19 coronavirus (the Toolbox) and the guidance to ensure compliance with data protection standards of apps fighting the pandemic (Data Protection Guidance, see further in this overview). This is the first tranche of measures announced by the European Commission in its Recommendation C(2020) 2296 on a common European Union approach for the use of technology and data to combat and exit from the Covid-19 coronavirus crisis, in particular concerning mobile applications and the use of anonymised mobility data (Recommendation, see further in this overview).</p>	<p>The press release about the Toolbox is available here.</p> <p>The Toolbox is available here.</p> <p>The press release about the data protection guidance is available here.</p> <p>The Data Protection Guidance is available here.</p> <p>The Recommendation is available here.</p>	<p>Mobile apps and new technology</p> <p>Cybersecurity and information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Toolbox aims to facilitate establishment of effective, interoperable app solutions throughout the EU that are based on privacy-enhancing technologies (PET), minimise the processing of personal data and support cross-border situations. To this end, the Toolbox covers in detail:</p> <ul style="list-style-type: none"> • essential apps requirements, including the epidemiological framework, technical functionalities, cross-border interoperability requirements and cybersecurity measures and safeguards; • measures to ensure accessibility and inclusiveness of the app solutions; • governance aspects, including the role of public health authorities in approving the tracing apps and measures to enable access by public authorities to apps-generated data; and • supporting actions, such as cooperation and sharing of epidemiological information between public health authorities, measures against harmful apps, and monitoring of the apps' effectiveness. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Apps with decentralised processing versus backend server solution</p> <p>The Toolbox discusses the privacy-preserving app solutions (already launched or still under development) that support public health efforts and minimise processing of personal data. The following two general categories are discussed:</p> <ul style="list-style-type: none"> • apps with decentralised processing, where proximity data related to contacts generated by the app remains only on the mobile device. The apps generate arbitrary identifiers of the phones that are in contact with the user and stores these identifiers on the user device, with no additional personal information or phone numbers. The provision of mobile phone numbers or other user's personal data at the time of the app installation is not necessary, because an alert is automatically delivered via the app the moment that a user notifies the app (with the approval of the health authority) that he/she has test positive. Public health authorities would not have access to any anonymised and aggregated information on 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>social distancing, on the effectiveness of the app or on the potential diffusion of the virus. An app might have an optional opt-in functionality allowing to share users their data with health authorities for further support and guidance;</p> <ul style="list-style-type: none"> • backend server solution, where the app functions through a backend server held by the public health authorities and used to store the arbitrary identifiers generated by the app. The data stored in the server can be anonymised by aggregation and further used by public authorities to analyse the intensity of contacts in the population, the effectiveness of the app in tracing and alerting contacts, and on the aggregated number of people that could potentially develop symptoms. Through the identifiers, users who have been in contact with a positively tested user will receive an automatic message or alert on their phone. An alerted person may choose to provide personal information to the public health authorities in order to get further support and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>guidance. In such a case, the user should express his/her consent.</p> <p>The Toolbox emphasises that none of these two options includes storing of unnecessary personal information. Options where directly-identifiable data on every person downloading the app is held centrally by public health authorities, would have major disadvantage, as noted by the EDPB in its response to consultation on the draft Guidance on Data Protection. Centralised storage of mobile phone numbers could also create risks of data breaches and cyberattacks.</p> <p>Cybersecurity</p> <p>The Toolbox addresses the cybersecurity risks most common for mobile apps and includes technical requirements to the apps (e.g. secure development practices, secure communication, the use of encryption and multi-factor user authentication). Annex 1 of the Toolbox lists best practices for app development and deployment compiled by ENISA. Requirements also include independent testing of the apps, access to source code and establishing policies for vulnerability handling and disclosure.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Toolbox further discusses measures aimed at ensuring adequate cybersecurity throughout the entire lifecycle of the apps (the app itself, the backend and any associated services). It recommends Member States carry out a national risk assessment to identify and mitigate possible risks of apps-related abuse and establish mechanisms for active cooperation with European and national CSIRTs on incident response and vulnerabilities disclosure.</p> <p>Next steps</p> <p>By 31 May 2020, Member States are to report to the European Commission on the actions taken and provide updates in their bi-weekly meetings for the duration of the pandemic. The European Commission will publish by 30 June 2020 a progress report and proposals for further follow-up actions.</p> <p>By the end of April 2020, the Member States and the European Commission will seek clarifications on the solutions proposed by Google and Apple on contact tracing functionality of the mobile operating systems (Android and iOS) and alignment of those solutions with the Toolbox requirements.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The European Commission expects to develop, by June 2020, a common approach for the use of anonymised and aggregated mobility data. The intended data use is (i) mapping and predicting the diffusion of the Covid-19 coronavirus, along with its impact on the national healthcare systems; and (ii) optimising the effectiveness of measures to contain the Covid-19 diffusion, confinement and de-confinement.</p>		
EU	European Commission	16/4/20	<p>European Commission issues data protection guidance on Covid-19 coronavirus contact tracing and warning apps</p> <p>The European Commission published a document setting out a common approach to the development, use and monitoring performance of mobile apps for tracing (the Toolbox, please see above) and guidance to ensure data protection compliance of apps fighting the pandemic (Data Protection Guidance).</p> <p>The guidance outlines the requirements that apps should fully comply with the requirements of the EU data protection, privacy and confidentiality of electronic communications laws (including the GDPR and ePrivacy Directive) and lists the following</p>	<p>The press release about the Toolbox is available here.</p> <p>The Toolbox is available here.</p> <p>The press release about the data protection guidance is available here.</p> <p>The Data Protection Guidance is available here.</p>	<p>Data protection-general guidance</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>elements to provide guidance on how to limit the intrusiveness of app functionalities:</p> <ul style="list-style-type: none"> • controllers: given the sensitivity of processing, national health authorities or entities carrying out tasks in the public interest in the field of health as controllers should be controllers in relation to the apps; • ensuring that individuals remain in control: the European Commission considers that this can only be achieved if the following conditions are met: <ul style="list-style-type: none"> ○ the installation of the app is genuinely voluntary and without any negative consequences for individuals that decide not to download or use it; ○ different app functionalities (e.g. information, symptom checker, contact tracing and warning functionalities) should not be bundled, so that individuals can provide their consent specifically for each functionality; ○ if proximity data are used, they should be stored on the individual's device 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and shared with health authorities only after confirmation that the individual is infected and upon individual's choice to do so;</p> <ul style="list-style-type: none"> ○ individuals should be provided with all necessary information about the processing of their personal data (in line with information requirements of the GDPR and ePrivacy Directive); ○ individuals should be able to exercise their data protection rights under the GDPR and any restrictions of their rights under ePrivacy Directive should be necessary, proportionate and provided for in the applicable national legislation; and ○ the apps should be deactivated at the latest when the pandemic is declared to be under control; the deactivation should not depend on de-installation by the user; <ul style="list-style-type: none"> ● legal basis for the data processing: installation of apps and the storing of 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>information on a user device can only be based on consent. National health authorities should typically be able to process personal data when there is a legal obligation laid down in EU or Member State law providing for such processing and meeting the conditions of Art.6(1)(c) and Art. 9(2)(i) GDPR or when such processing is necessary for the performance of a task carried out to further the public interest recognised by EU or Member State law;</p> <ul style="list-style-type: none"> • data minimisation: an assessment of the need to process personal data and the relevance of such personal data should be conducted in the light of the purpose(s) pursued. The European Commission recommends using Bluetooth Low Energy communications data (or data generated by equivalent technology) to determine proximity and states that location data are not necessary for the purpose of contact tracing functionalities and processing of location data in the context of contact tracing would be difficult to justify in the light of data 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>minimisation principle and might create security and privacy issues;</p> <ul style="list-style-type: none"> • limiting disclosure and access of data: the European Commission discusses the limits of using data related to symptom checker and telemedicine functionality and in relation to contract tracing and warning. For the latter, the guidance recommends using the decentralised solution as being more in line with the principle of data minimisation; • precise purposes for processing should be provided, there may be several purposes for each functionality of the app. In this case, the European Commission recommends not bundling different functionalities and providing choice. For contact tracking functionality, the recommended wording could be "retaining of the contacts of the persons who use the app and who may have been exposed to infection by COVID-19 in order to warn those persons who could have been potentially infected"; • setting strict data storage limits: for contact tracing and warning apps, proximity data 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>should be deleted as soon as possible and within maximum one month (incubation period plus margin) or after the person was tested and the result was negative;</p> <ul style="list-style-type: none"> • ensuring data security: to achieve this end, the recommendation is to: <ul style="list-style-type: none"> ○ store data on the user's device using state-of-the art encryption; ○ if data is stored in central server, access logging should be in place; ○ store proximity data in encrypted and pseudonymised format; ○ publish and make available for review the source code of the app; and ○ all transmissions of data to health authorities should be encrypted. 		
EU	European Commission	8/4/20	<p>European Commission proposes a pan-European approach for the use of mobile data in response to the Covid-19 Coronavirus pandemic</p> <p>The European Commission issued a Recommendation proposing measures to develop a</p>	<p>The press release is available here.</p> <p>The Recommendation is available here.</p>	<p>Mobile apps and new technology</p> <p>Data processing-location data</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>common European Union approach for the use of technology and data to combat and exit from the Covid-19 coronavirus crisis, in particular concerning mobile applications and the use of anonymised mobility data (the Toolbox). The Recommendation includes:</p> <ul style="list-style-type: none"> • a common approach for the use of mobile applications, coordinated at EU level, that will be used for: <ul style="list-style-type: none"> ○ enabling individuals in the EU to take effective and more targeted social distancing measures; ○ warning, preventing and contact tracing for curbing the propagation of the Covid-19 disease; • a methodology for monitoring and sharing assessments of effectiveness of these apps, their interoperability and cross-border implications, and their respect for security, privacy and data protection; • a common scheme for using anonymised and aggregated data on mobility of populations, for the purposes of: <ul style="list-style-type: none"> ○ modelling and predicting the evolution of the disease; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ monitoring the effectiveness of national measures such as social distancing and confinement; and, ○ formulating a coordinated strategy for exiting from the Covid-19 crisis. <p>The European Commission urges EU member states to ensure that all actions in this respect are taken in accordance with the EU and national law, in particular laws on medical devices and the right to privacy and the protection of personal data along with other rights and freedoms enshrined in the EU Charter of Fundamental Rights. The Recommendation includes proposals for safeguards to privacy and data protection applicable in this context.</p> <p>The European Commission intends to publish the pan-European approach for Covid-19 mobile applications on 15 April 2020 and will complement it by providing practical guidance on the data protection and privacy implications of the use of mobile warning and prevention apps. It requests the member states to start sharing information on current and intended apps for peer review immediately and proposes a maximum one-week period for commenting on such intended uses.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The first report on the effects of the Recommendation is expected in June 2020.		
EU	European Commission, European Parliament, Council of the European Union	23/4/20	<p>Date of application of the EU Medical Devices Regulation postponed due to the Covid-19 coronavirus pandemic</p> <p>The European Parliament and the Council of the European Union have adopted by urgent procedure the proposal of the European Commission to postpone the application date of the Medical Devices Regulation (Regulation (EU) 2017/745) (MDR) until 26 May 2021 and to postpone the date of repeal of Council Directive 90/385/EEC on active implantable medical devices. The proposal will not affect the date of application of the In Vitro Diagnostics Medical Devices Regulation, due to become applicable from 26 May 2022.</p> <p>The decision is intended to prevent unnecessary shortages and delays in medical equipment supplies during the Covid-19 coronavirus pandemic, primarily due to authorities and conformity assessment bodies attempting to implement the MDR and the need of medical device manufacturers to comply with higher security standards The Regulation amending the</p>	<p>The notification about postponed application is available here.</p> <p>The Regulation amending MDR is available here.</p> <p>The press release of the European Parliament is available here.</p> <p>The press release of the European Commission is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			MDR was published in the Official Journal of the EU on 23 April 2020 and came into force immediately.		
EU	European Commission	24/3/20	<p>European Commission discusses with telecom companies sharing of anonymised data for modelling and predicting the progress of the Covid-19 coronavirus</p> <p>The European Internal Market Commissioner Thierry Breton held a videoconference with European telecoms operators and the GSMA, an association of mobile telecommunications providers, where he discussed, amongst other things, the need to collect and share with the European Commission, anonymised mobile metadata to assist in assessing progression of the Covid-19 coronavirus. The European Commission stressed that processing this data should be done in a way that is fully compliant with the GDPR and ePrivacy legislation.</p> <p>The intended data processing raised many concerns amongst commentators about any collection of such data, their anonymisation, the usefulness of information, and the risks to privacy and other fundamental rights and freedoms of individuals. Some</p>	The statement regarding this call is available here .	Data processing- location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of these concerns were voiced by the European Parliament Member Sophia in 't Veld.</p> <p>In response to MEP in 't Veld concerns, the Commissioner Breton confirmed on 26 March that anonymisation would be used and that data would be deleted but no specific detail was provided.</p> <p>Please also see below the response of the European Data Protection Supervisor Wojciech Wiewiórowski.</p> <p>The videoconference also discussed network resilience and the importance of protecting the networks against cyberattacks.</p>		
EU	European Data Protection Board (EDPB)	28/4/20	<p>EDPB reiterates that the GDPR adequately covers data protection in the context of the Covid-19 coronavirus pandemic and summarises its recent guidance</p> <p>The EDPB published its responses to recent requests of the members of the European Parliament (MEPs) on the applicability of data protection laws and guidance on data privacy and data protection in relation to the Covid-19 Coronavirus pandemic.</p> <p>In the letter to MEPs Ďuriš Nicholsonová and Jurzyca, the EDPB clarified that data protection laws already</p>	<p>The overview of adopted documents is available here.</p> <p>The press release is available here.</p> <p>The letter to MEPs Ďuriš Nicholsonová and Jurzyca is available here.</p>	<p>Data protection – general guidance</p> <p>Data processing – location data</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>take into account data processing operations necessary to contribute to the fight against an epidemic and therefore it is not necessary to enhance GDPR provisions but just to observe them. The EDPB noted that the rights and responsibilities of national health authorities in relation to processing personal data during the pandemic depend largely on the relevant Member State's law. Similarly, national labour laws determine what employers are allowed to do in relation to their personnel.</p> <p>The letter refers to data protection guidance in relation to the pandemic issued by the EDPB to date, namely:</p> <ul style="list-style-type: none"> • two statements of the EDPB of 16 and 19 March 2020, discussing general considerations that should be taken into account so that lawful processing of personal data is ensured and data protection principles are respected during the pandemic; • the 21 April guidelines on the issues of geolocation and other tracing tools (<i>see further in this overview</i>); and 	<p>The letter to MEP Sophia in 't Veld is available here.</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> the 21 April guidelines on the processing of health data for research purposes (<i>see further in this overview</i>). <p>The EDPB reiterates that the principles of data protection law (such as lawfulness, transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation and security) serve a dual purpose, namely to guarantee the protection of fundamental rights of citizens and to create trust in the governments that are looking into post-confinement data driven measures.</p> <p>Requirements of data protection law in relation to transparency and data quality can play a key role in public acceptance of any Covid-19 coronavirus-related measures enacted by governments and the take-up of voluntary initiatives proposed by private entities.</p> <p>The statements and guidance issued by the EDPB to date are also highlighted in the letter in response to several questions on technological developments to fight the spread of Covid-19 coronavirus submitted by the MEP Sophia in 't Veld.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	European Data Protection Board (EDPB)	28/4/20	<p>EDPB highlights cross-border transfer options for scientific research purposes</p> <p>The EDPB published a letter responding to questions of the US Mission to the EU on the transfer of personal data for the purpose of scientific research and the development of vaccines and treatments to combat Covid-19 coronavirus. The US Mission enquired about the possibility of relying on a derogation of Art. 49 GDPR to enable international data flows.</p> <p>The EDPB referred to guidance provided in its new Guidelines 03/2020 on the processing of health data for scientific research, adopted on 21 April 2020 (see <i>further in this overview</i>).</p> <p>The press release discussing the letter emphasises that the GDPR allows for collaboration between EEA and non-EEA scientists. Solutions for cross-border data transfers outside the EEA that guarantee the continuous protection of data subjects' fundamental rights, such as adequacy decisions or appropriate safeguards, should be favoured. However, in the absence of an adequacy decision or appropriate safeguards, public authorities and private entities may also rely upon derogations included in Art. 49 GDPR.</p>	<p>The press release is available here.</p> <p>The letter to the US Mission to the EU is available here.</p>	<p>Data processing – scientific research</p> <p>Data processing – public authorities</p> <p>Cross-border data transfers</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The EDPB considers that the fight against Covid-19 coronavirus has been recognised by the EU and Member States as an important public interest, as it has caused an exceptional health crisis of an unprecedented nature and scale. In this light, the urgent action in the field of scientific research may necessitate transfers of personal data to third countries or international organisations.</p> <p>In the press release about the letter, the Chair of the EDPB Andrea Jelinek reiterates that the GDPR is flexible enough to offer faster temporary solutions for cross-border data transfers in the face of the urgent medical situation.</p>		
EU	European Data Protection Board (EDPB)	21/4/20	<p>EDPB adopts guidelines on geolocation and other tracing tools in the context the Covid-19 coronavirus outbreak</p> <p>The guidelines clarify the conditions and principles of processing for two specific purposes:</p> <ul style="list-style-type: none"> • using location data to model the spread of the virus and assess the effectiveness of confinement measures; and • contact tracing to notify individuals that they have been in close proximity to a confirmed carrier of the virus. 	<p>The press release is available here.</p> <p>The guidelines are available here.</p>	<p>Data processing – location data</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The EDPB reiterates its earlier position that the use of contact tracing apps should be voluntary and should not rely on tracing individual movements but instead on proximity data.</p> <p>The guidance notes that the GDPR and the ePrivacy Directive contain specific rules allowing for the use of anonymous or personal data to support public authorities in monitoring and containing the spread of the Covid-19 coronavirus, for example through processing of location data.</p> <p>Derogations to the ePrivacy Directive are possible on basis of national law where they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives. Re-use of location data collected by a telecom service provider to model the outbreak's spread is possible if additional conditions are met, such as the data subject's additional consent under the specific national law.</p> <p>The EDPB emphasises that wherever possible processing should be of anonymised, rather than personal data. Furthermore, it notes that while anonymisation removes processing restrictions,</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>pseudonymised data remains within the scope of the GDPR.</p> <p>Techniques applied to anonymise personal data should prevent the possibility of linking the data with an identified or identifiable natural person with any "reasonable" effort. This takes into account objective aspects (including time and technical means) and contextual elements (such as the population density, rarity of a phenomenon, nature of data or their volume). To achieve the anonymisation of location data, whole location datasets should be considered and the data of a large set of individuals should be processed. The EDPB notes that location data remains difficult to anonymise.</p> <p>The annex to the guidelines includes a detailed guide for contact tracing apps aimed at app designers and implementers.</p>		
EU	European Data Protection Board (EDPB)	21/4/20	<p>EDPB adopts guidelines on the processing of health data for research purposes in the context of the Covid-19 coronavirus outbreak</p> <p>The EDPB adopted the guidelines on the processing of data concerning health for the purposes of scientific research in the context of the pandemic. The EDPB</p>	<p>The press release is available here.</p> <p>The guidelines are available here.</p>	<p>Data processing – scientific research</p> <p>Data processing – public authorities</p> <p>Cross-border data transfers</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>points out that the Covid-19 coronavirus pandemic causes an exceptional health crisis of an unprecedented nature and scale and the EDPB considers that the fight against Covid-19 coronavirus has been recognised by the EU and most of its Member States as an important public interest which may require urgent action in the field of scientific research (for example to identify treatments and/or develop vaccines), and may also involve transfers to third countries or international organisations.</p> <p>The guidelines clarify in detail the following:</p> <ul style="list-style-type: none"> • special rules for the processing of health data for the purpose of scientific research under the GDPR are also applicable in the context of the Covid-19 coronavirus pandemic; • the conditions for and the extent of such processing may differ per EU member state, as national legislators have discretion to adopt special laws in accordance with Art. (9)(2)(i) and (j) GDPR to enable the processing of health data for scientific research purposes. Processing of health data for the purpose of scientific research must also rely on one of the 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>legal bases in Art. 6 (1) GDPR. The guidance addresses processing based on data subject consent. One of the examples of when data subject's consent can be used as the basis for processing is processing related to a survey of symptoms and progress of the Covid-19 coronavirus conducted as part of a non-interventional study on a given population (taking into account the obligations of Art.7 GDPR), as the EDPB does not consider this example as a case of "clear imbalance of power". The data subjects should not be in a situation of dependency on the researchers that could inappropriately influence the exercise of their free will and it should be clear that refusing consent will have no adverse consequences;</p> <ul style="list-style-type: none"> all national laws enacted on the basis of Art.(9)(2)(i) and (j) GDPR must be interpreted in the light of the principles relating to processing personal data provided in Art. 5 GDPR and take into account the jurisprudence of the Court of Justice of European Union. The EDPB reiterates that any such derogations 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and limitations in relation to the protection of data must apply only in so far as is strictly necessary;</p> <ul style="list-style-type: none"> • specific attention should be given to ensuring appropriate security of the personal data in the context of the Covid-19 coronavirus outbreak, including protection against unauthorised or unlawful processing and against incidental loss, destruction or damage, putting appropriate technical and organisational measures in place, such as pseudonymisation and encryption of data and security measures for systems and services stipulated in Art. 32(1) GDPR and safeguards under Art.89 (1) GDPR; • there must be an assessment made whether a DPIA pursuant to Art.35 GDPR has to be carried out; • storage periods (timelines) must be set and must be proportionate, taking into account criteria such as the length and the purpose of the research. Rules on storage periods may also be stipulated in national laws; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> the Covid-19 coronavirus outbreak does not suspend or restrict data subjects exercising their rights under Art.12-22 GDPR, however, national legislators may restrict some of these rights in accordance with Art.89(2) GDPR; international data transfers of health data for scientific research purposes in the context of the pandemic are subject to the general requirements to cross-border data transfers under the GDPR. The EDPB discusses options available in the absence of an adequacy decision or other appropriate safeguards and notes that, in exceptional cases, public authorities and private entities may rely on the applicable derogations under Art.49 GDPR. 		
EU	European Data Protection Board (EDPB)	17/4/20	<p>EDPB responds to European Commissions data protection guidance for Covid-19 coronavirus apps</p> <p>The EDPB published a letter in response to the European Commission's draft Data Protection Guidance for apps designed to help fight Covid-19 coronavirus.</p>	<p>The press release is available here.</p> <p>The EDPB letter is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The EDPB confirms its support for the European Commission's proposal for voluntary adoption of these apps, but notes that this does not necessarily mean the processing by public authorities can be based on an individual's consent. The EDPB states the most relevant legal basis for personal data processing in this respect will be necessity for the performance of a task for public interest. The EDPB notes that a legal basis for the use of the apps can be provided in newly enacted national laws that would promote the voluntary use of the app without any negative consequences for individuals not using the apps or uninstalling the apps at will.</p> <p>The EDPB letter addresses the proposed use of contact tracing and the warning function within the apps. The EDPB notes that contact tracing does not require location tracking, and collecting the individual's movements would violate the principle of data minimisation and create major privacy risks. Instead, contact tracing should discover events (contacts with positive persons) as defined by health authorities and scientists. The circumstances of when events are shared should be controlled by a strict necessity test as required by law. The EDPB</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>suggests that both the centralised and the decentralised storage of these contacts could be valid options, provided that adequate security measures are in place. The EDPB notes that the decentralised solution would be more aligned with the data minimisation principle.</p> <p>The EDPB suggests the warning function must not spread social alarm or enable stigmatisation of individuals. Implementation of an in-app notification for informing individuals may envisage that the app processes random pseudonyms. The EDPB advocates a call back mechanism to a human agent for those that receive a positive notification, and no other potential identifying element of the data subject should be included in this advice to prevent re-identification of any persons. No directly identifying data should be stored in the users' device, and any such data should be erased as soon as possible.</p> <p>The EDPB agrees with the European Commission that any data collected from these apps should be erased or anonymised once the crisis is over. The EDPB emphasised that the EDPB itself and national supervisory authorities that are in charge of advising on the application of the GDPR and the e-Privacy</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			Directive should be engaged in the process of implementing these measures.		
EU	European Data Protection Board (EDPB)	7/4/20	<p>EDPB commits to swiftly issuing Covid-19 guidance on geolocation and tracing tools and on processing of health data for research purposes</p> <p>The EDPB published a press release clarifying that expert subgroups of the EDPB will develop guidance on the following aspects of personal data processing in relation to the Covid-19 Coronavirus:</p> <ul style="list-style-type: none"> • geolocation and other tracing tools in the context of the Covid-19 outbreak, covering the following issues: <ul style="list-style-type: none"> ○ the use of aggregated/anonymised location data (e.g. provided by telecoms service providers) and the effectiveness of aggregation and anonymisation techniques; ○ how the principles of lawfulness, necessity, proportionality, accuracy, and data minimisation apply to different methods to gather location data or trace interactions between individuals; 	<p>The press release is available here.</p> <p>The mandate for developing guidance on geolocation and other tracking tools is available here.</p> <p>The mandate for guidance on processing health data for research purposes is available here.</p>	<p>Data processing – location data</p> <p>Mobile apps and new technology</p> <p>Data processing– scientific research</p> <p>Data processing – public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ general legal analysis of the use of apps and collection of personal data by apps to help contain the spread of the virus; ○ safeguards to ensure compliance with data protection principles in the context of using geo-location or other tracing tools; ○ recommendations or functional requirements for contact tracing applications; ○ ensuring that such measures are limited to what is strictly necessary to tackle the emergency situation and must be lifted once the pandemic is over; ● processing of health data for research purposes in the context of the Covid-19 outbreak, covering the following issues: <ul style="list-style-type: none"> ○ processing of health data for the purpose of advancing scientific and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>medical research connected to the Covid-19 coronavirus crisis;</p> <ul style="list-style-type: none"> ○ legal basis, the principle of proportionality, information and exercise of the rights of data subjects (right to object, right to erasure, etc.), retention period etc.; ○ re-use of medical research data connected to the Covid-19 crisis and data sharing; ○ information and exercise of the rights of data subjects in an emergency situation. <p>The EDPB noted that it has postponed work on earlier announced guidance on teleworking tools and practices in the context of the Covid-19 outbreak in order to be able to prioritise the above topics.</p> <p>The EDPB Chair Andrea Jelinek said the EDPB to move swiftly to issue guidance as soon as possible, to help make sure that technology is used in a responsible way to support the battle against the pandemic.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	European Data Protection Board (EDPB)	20/3/20	<p>EDPB releases a statement on the processing of personal data in the context of Covid-19 coronavirus</p> <p>The EDPB released a statement on the processing of personal data in the context of the Covid-19 coronavirus outbreak addressing processing by competent public health authorities and private employers. The EDPB guidance addresses the following main issues:</p> <ul style="list-style-type: none"> <i>Lawfulness of processing in an employment context.</i> The EDPB clarifies that employers may process personal data where necessary for compliance with their legal obligations or for the public interest and that national or European Union law may also provide derogations for processing special categories of personal data on the basis of substantial public interest in the area of public health (Art. 9(2)(i) GDPR), or to protect the vital interests of the individual (Art.9(2)(c) GDPR). Individuals should be provided with information about the main features of processing, retention period and purpose. Adequate security measures and confidentiality policies should be adopted and decisions documented. 	The statement is available here .	Data processing-employment Data processing-public authorities Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • <i>Can an employer require visitors or employees to provide specific health information in the context of the Covid-19 coronavirus?</i> The employer should only require health information to the extent that national law allows it. • <i>Is an employer allowed to perform medical check-ups on employees?</i> This depends on national law: employers should only access and process health data if required by law. • <i>Can an employer disclose that an employee is infected with the Covid-19 coronavirus to his colleagues or to externals?</i> Employers should inform staff about the Covid-19 coronavirus cases and take protective measures, but should not communicate more information than necessary. 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, concerned employees must be informed in advance and their dignity and integrity protected. • <i>What information processed in the context of Covid-19 coronavirus can be obtained by the employers?</i> Employers may obtain personal 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>information to fulfil their duties and to organise the work in line with national legislation.</p> <ul style="list-style-type: none"> • <i>In relation to processing location data:</i> <ul style="list-style-type: none"> ○ <i>Lawfulness of processing of telecom data, including location data.</i> The EDPB clarifies that national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals. The EDPB reiterates that Art. 15 of the ePrivacy Directive enables Member States to introduce exceptional legislation to safeguard public security, however, this legislation must constitute a necessary, appropriate and proportionate measure within a democratic society. And in case of an emergency, it should also be strictly limited to the duration of the emergency at hand. ○ Governments of some EU Member States consider using mobile location data for monitoring, containing or mitigating the spread of Covid-19 coronavirus, e.g. by 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>locating individuals or sending public health messages to telephones of individuals in a specific area. The EDPB recommends that public authorities first seek to process geolocation data in an anonymous way, as personal data protection rules do not apply to data which has been appropriately anonymised. If not possible, the ePrivacy Directive includes provisions that allow adoption by Member States of legislative measures to safeguard public security (Art. 15 ePrivacy Directive). Such measures are subject to proportionality test and require putting in place adequate safeguards and ensuring a right to a judicial remedy.</p>		
EU	<p>European Data Protection Supervisor (EDPS) [Updated as at 21 May 2020]</p>	8/5/20	<p>EDPS publishes blogs regarding data protection and privacy during the Covid-19 coronavirus crisis</p> <p>In the 30 April blog, the EDPS considers that laws, such as the GDPR and the e-Privacy rules, allow for the processing of personal data for public health purposes, and data protection law is well-equipped to support the fight against the Covid-19 coronavirus.</p>	<p>The 8 May blog is available here.</p> <p>The 30 April blog is available here.</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>However, the EDPS urges high levels of regulatory scrutiny and foresight with consideration given to "where to draw the line", as may be specified by law but also ethics. The EDPS:</p> <ul style="list-style-type: none"> • provides examples for consideration such as, how long will measures be applied/intrusion in rights and freedoms last? will re-use of data be for the public good and what does that mean? • highlights the current digital business model, including endemic tracking, and notes how he considers that the current crisis may amplify its impact (imbalance of power and information; insufficient transparency and accountability; growing inequality; role of platforms; cybersecurity incidents and disinformation campaigns). • considers the need for a sustainable "new normal" (including in the digital realm) and how this crisis may be an opportunity to address growing inequalities, online unfair treatment, and discrimination. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> plans a careful analysis of long-term implications of the pandemic for fundamental rights and freedoms, to be finalised by the end of the year. <p>On 8 May the EDPS published a blog reporting on the first international meeting of the DPOs of EU institutions and bodies:</p> <ul style="list-style-type: none"> highlighting the establishment of a Covid-19 Task Force to assist those institutions and bodies in their response to the crisis; encouraging a pan-EU approach in which data and technology can help to solve the crisis; and championing the use of data for the good of all through responsible processing. 		
EU	European Data Protection Supervisor (EDPS)	7/5/20	<p>EDPS gives the introductory speech at the "Exchange of views with the LIBE Members on the use of personal data in the fight against Covid-19"</p> <p>Giving a speech to the LIBE Members, Wojciech Wiewiórowski, the EDPS, called for EU digital solidarity and a pan-European approach to the pandemic. He noted that independent oversight and</p>	The EDPS speech is available here .	Data protection-general guidance. Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>guidance are even more essential for data protection in times of crisis, when we can measure commitment to values, but considered that data protection is part of the Covid-19 coronavirus solution and not the problem.</p> <p>He went on to discuss recent EDPS activity in relation to the crisis, the use of a various mobile apps to tackle the pandemic, provided an explanation of contact tracing and flagged the inevitable "second wave" of personal data debate in the context of the Covid-19 coronavirus.</p>		
EU	European Data Protection Supervisor (EDPS)	7/5/20	<p>EDPS publishes a TechDispatch regarding contact tracing mobile apps in the context of the Covid-19 coronavirus outbreak</p> <p>The EDPS TechDispatch sets out what is meant by contact tracing, both traditionally and digitally, the nature of the technology and in particular, data protection points of note including:</p> <ul style="list-style-type: none"> • risk of large scale surveillance and user identification (through combination of app related information and other data such as location of specific individuals), and the consequent need for data minimisation, 	The TechDispatch is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>pseudonymised data, avoidance of location data and application of safeguards preventing re-identification;</p> <ul style="list-style-type: none"> • need for data protection by design for centralised and decentralised models of contact tracing app; • need to apply purpose limitations and associated methods to prevent collection of identifiers post-crisis and delete collected data; • need for transparency; • risk of poor data accuracy and integrity (false positives/negatives); and • risk to security of personal data through radio wave disruption by adversaries. 		
EU	European Data Protection Supervisor (EDPS)	27/4/20	<p>EDPS published its answers on data protection issues in the context of the Covid-19 coronavirus outbreak</p> <p>Wojciech Wiewiórowski, the EDPS, has published his introductory remarks and detailed Q&A on various data protection aspects of combatting the Covid-19</p>	<p>The Q&A is available here.</p> <p>The introductory remarks are available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-location data</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>coronavirus, provided to the Committee for European Affairs of the Senate of the Republic of France.</p> <p>The Q&A addresses numerous issues, including the following;</p> <ul style="list-style-type: none"> • the regulatory landscape applicable to processing personal data in relation to the pandemic; • the European Commission's Toolbox; • detailed consideration of various aspects of the contact tracing apps and other technological developments aimed at containing the pandemic; • consideration of possible geo-tracking of individuals; • reflection on the opinion regarding mobile apps issued by the CNIL and on the so-called Robert information protocol proposed by French and German researchers for tracing Covid-19 coronavirus infections; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> data retention, data erasure and keeping data for research purposes after the epidemic, including data anonymisation aspects. 		
EU	European Data Protection Supervisor (EDPS)	6/4/20	<p>EDPS calls for a pan-European approach against the Covid-19 coronavirus outbreak</p> <p>Wojciech Wiewiórowski, the EDPS, has published a video address where he notes that numerous projects arising in the EU member states to tackle the Covid-19 coronavirus pandemic, by developing mobile applications, use different approaches to protecting public health and often involve personal data processing.</p> <p>The EDPS discusses risks inherent to such diverging approaches and calls for a pan-European model "Covid-19 mobile application" that would be coordinated at an EU level. The EDPS expresses its full commitment to cooperating with other European Institutions to implement technological solutions in a data protection-compliant way as soon as possible.</p> <p>The EDPS emphasises that any solutions (including technological, organisational and legal ones) must comply with the principle that personal data may only be processed for specified legitimate purposes, where</p>	The video address is available here and the transcript of the speech is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>necessary for these purposes, and not used in a way incompatible with those purposes.</p> <p>The EDPS has further clarified the following:</p> <ul style="list-style-type: none"> the GDPR allows sensitive data, including health data, to be processed when this is necessary for reasons of substantial public interest in the area of public health, such as protecting against serious cross-border threats to health, provided the basis of EU or member state law must be proportionate to the aim pursued; the EDPS is going to work with the European Commission to ensure that any measures taken at an EU level or national level are temporary and their purposes are limited. Furthermore, access to the data should be limited and it must be clear what will be done with the raw data used and with the results of intended operations; technology developers currently creating mobile applications to combat the Covid-19 coronavirus outbreak must have data protection principles, such as data protection 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>by design, engrained in the development from the start; and</p> <ul style="list-style-type: none"> the EDPS are working closely with data protection authorities in a wide range of jurisdictions, both in the European Economic Area and outside of the EU. 		
EU	European Data Protection Supervisor (EDPS)	25/3/20	<p>EDPS responds to the European Commission on data protection aspects of telecom data sharing in the context of Covid-19 coronavirus</p> <p>In the context of EDPS awareness of discussions between some Member States with telecommunications providers regarding use of data to track the spread of the Covid-19 coronavirus, the EDPS confirmed his view that "data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics".</p> <p>The EDPS raised a number of points for the European Commission's consideration regarding the use of data to track movements of people and the progression of the Covid-19 coronavirus, including:</p>	The letter is available here .	Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • European Commission's plans to use anonymised data would fall outside the scope of data protection rules but: <ul style="list-style-type: none"> ○ anonymisation involves more than simply removing identifiers (such as phone numbers and International Mobile Equipment Identity numbers); • data aggregation was another additional safeguard envisioned by the European Commission; • any data model used for exchange of data should ensure the European Commission can respond to the needs of the users of these analyses; • the dataset the European Commission wants to obtain should be clearly defined; • the European Commission should ensure full public transparency; • information security obligations under Commission Decision 2017/464 still apply, as do confidentiality obligations under the Staff 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Regulations for any European Commission staff processing the information;</p> <ul style="list-style-type: none"> • third parties used to process data must apply equivalent security measures and be bound by strict confidentiality obligations and prohibitions on further data use; • adequate measures to ensure the secure transmission of data from the telecom providers should be in place; • access to the data should be limited to authorised experts in spatial epidemiology, data protection and data science; • data obtained from mobile operators should be deleted as soon as the current emergency comes to an end and the "special services" should be deployed temporarily because of this specific crisis; • this solution should be considered extraordinary with scope to step back; • the European Commission's Data Protection Officer should be engaged throughout the entire process to provide assurance that the 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>data processed has indeed been effectively anonymised.</p> <p>The EDPS requested a copy of the data model, once defined, for information and noted that if the modalities for processing changed, a new consultation of the EDPS would be necessary.</p>		
EU	European Banking Authority (EBA)	22/4/20	<p>EBA publishes statement on additional supervisory measures relevant during the Covid-19 coronavirus outbreak</p> <p>The EBA has published a statement on supervisory measures it will employ in the context of the Covid-19 coronavirus crisis.</p> <p>Specifically, the statement provides further detail on the EBA's supervisory approach and the principles of effectiveness, flexibility, and pragmatism that guide it. This approach is called out as being relevant to Supervisory review and Evaluation Process (SREP), Recovery Planning, Digital Operational resilience and the application of the Guidelines on payment moratoria to securitisations.</p> <p>With regards to operational resilience, the statement highlights its importance in order to ensure business continuity, adequate information and communication</p>	<p>The press release is available here.</p> <p>The statement is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>technology capacity, security risk management, and to prevent cybercrime. It recognises that challenges faced by financial institutions in providing most services online whilst the number of home working staff has increased and customers become reliant on remote services</p> <p>The EBA considers that its new ICT and security risk management Guidelines applicable from June 2020 will form part of operational resilience, setting out requirements for certain financial institutions in the EU (credit institutions, investment firms and payment service providers) in relation to the mitigation and management of their ICT and security risks including the need for cybersecurity within a financial institution's information security measures.</p> <p>Given that financial institutions are required to make every effort to comply with EBA Guidelines: the EBA calls on financial institutions to:</p> <ul style="list-style-type: none"> ensure they have adequate internal governance and control framework (including firm-wide risk management framework) for operational resilience (business continuity, ICT and security risks management), including 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>involvement of management in effective decision-making and priority setting;</p> <ul style="list-style-type: none"> • ensure appropriate ICT and security risk management, focusing on mitigation of the most significant ICT risks, management of areas such as information security and monitoring, ICT operations and business continuity management (including third party providers), taking into account the evolving environment; • take the necessary measures to ensure the capacity of their IT systems support their most critical activities, including those enabling their customers to carry out their operations remotely; • stay vigilant in cyber security monitoring and measures, as the current situation might pose additional cyber threats; • ensure effective crisis communication measures with all relevant stakeholders, including with customers in light of potential additional cyber crime activities or operational disruptions; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • monitor and seek assurance as to compliance of third party providers with the financial institution's security objectives, measures and performance targets; • ensure that the business continuity plans are up to date and adapted, including considerations related to potentially longer-term nature of the measures applied for Covid-19 coronavirus crisis. <p>The EBA:</p> <ul style="list-style-type: none"> • calls on competent authorities to work closely with their supervised institutions to ensure effective prioritisation of efforts in accordance with the principle of proportionality and to apply reasonable supervisory flexibility when assessing the implementation of the Guidelines; • suggests that supervisory attention and support could be focused on the provisions relating to information security, ICT operations and business continuity management (where financial institutions should aim to maximise their abilities to provide services on an 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			ongoing basis and to limit losses in the event of severe business disruption).		
EU	European Insurance and Occupational Pensions Authority (EIOPA)	17/4/20	<p>EIOPA issues statement on mitigating the impact of Covid-19 coronavirus pandemic on the occupational pensions sector</p> <p>EIOPA published a statement addressed to national competent authorities on mitigating the impact of the Covid-19 coronavirus pandemic, noting, amongst other things, that the Institutions for Occupational Retirement Provision (IORPs) should consider business continuity and operational risk.</p> <p>EIOPA expects national competent authorities to adhere to certain principles using a risk-based and proportionate approach including amongst other things expecting IORPs to carefully consider and effectively manage the increased risk exposure to fraud, other criminal activity, cyber security and data protection due to the disruption of society and, in particular, staff working remotely.</p>	<p>The press release is available here.</p> <p>The statement is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	EUROPOL	3/4/20	<p>EUROPOL issues a report addressing cybersecurity risk in the context of the Covid-19 coronavirus</p> <p>EUROPOL notes that it has been monitoring the impact of the Covid-19 coronavirus on the cybercrime landscape and has published, in the form of a report, an updated threat assessment of potential further developments in this crime area.</p> <p>This includes analysis regarding:</p> <ul style="list-style-type: none"> • ransomware; • DDoS; • child sexual exploitation; • the dark web; • hybrid threats: disinformation and interference campaigns. 	The report is available here .	Cybersecurity and information security
EU	European Commission European Union Agency for	20/3/20	<p>The European Commission, ENISA, Europol, and CERT-EU issue a statement on the Covid-19 coronavirus outbreak</p> <p>The European Commission, ENISA, Europol, and CERTEU issued a joint statement to highlight that they are coordinating efforts to track potential</p>	The European Commission's press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
	<p>Cybersecurity (ENISA)</p> <p>Computer Emergency Response Team for the EU Institutions (CERT EU)</p> <p>European Union Agency for Law Enforcement Cooperation (Europol)</p>		malicious cyber activities in the context of an increased number of people working from home during the Covid-19 coronavirus outbreak.	<p>ENISA's press release is available here.</p> <p>Europol's press release is available here.</p>	
EU	EU Agency for Cybersecurity (ENISA) [Updated as at 21 May 2020]	18/5/20	<p>ENISA issues recommendations on security of smart infrastructure during the Covid-19 Coronavirus crisis</p> <p>ENISA highlighted in its recommendations that the cybersecurity of smart homes and smart buildings is more relevant that ever during the Covid-19 coronavirus outbreak.</p> <p>It suggests, with regards to home premises (where many currently work):</p>	The press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • using multiple passwords, multi-factor authentication and biometric and PIN features; • following security features, applying updates, enabling notifications; • avoiding introducing sensitive information and being aware of information used; and • configuring and separating networks, turning off devices when not in use and wiping before disposal/return. <p>With regards to business premises, amongst other things:</p> <ul style="list-style-type: none"> • enabling firewall protection; • disabling unused ports; • applying network micro-segmentation by creating virtual networks to isolate Internet of Things systems from other critical IT systems; and • preparing and updating incident response plans according to the current risks. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	EU Agency for Cybersecurity (ENISA)	11/5/20	<p>ENISA issues cybersecurity advice to support hospitals and the healthcare sector against the increase of phishing campaigns and ransomware attacks during the Covid-19 coronavirus pandemic</p> <p>ENISA highlights the redirection of resources to the primary healthcare goal as creating vulnerability in the healthcare sector with risk exacerbated by:</p> <ul style="list-style-type: none"> • high demand for certain goods like protective masks, disinfectants and household products; • decreased mobility and border closures; • increasing reliance on teleworking, often with little previous experience and planning; and • increased fear, uncertainty and doubt in the general population. <p>As such, ENISA recommends:</p> <ul style="list-style-type: none"> • sharing vulnerability information with healthcare staff, building awareness of the situation (including through campaigns) and, in the case of cyber infection, asking staff to 	The advice is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>disconnect from the network to contain the spread;</p> <ul style="list-style-type: none"> • if a system is compromised, freezing any activity in the system and disconnecting infected machines, going offline and contacting the national CSIRT; • ensuring effective back up, restoration procedures and business continuity plans; • coordinating with manufacturers if medical devices affected; and • segmenting networks. 		
EU	EU Agency for Cybersecurity (ENISA)	6/5/20	<p>ENISA publishes recommendations regarding phishing during the Covid-19 coronavirus outbreak</p> <p>In general advice, ENISA recommended the following to mitigate against phishing attacks (with respect to which people and organisations are particularly vulnerable given reliance on email for communications):</p> <ul style="list-style-type: none"> • reflect on a request for your personal information and whether appropriate; 	The press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • never provide personal or financial information or passwords via email; • avoid emails that insist you act now; • look at wording and terminology to ensure it reflects usual expectations/usage and does not raise suspicions; • check the email address and sender’s name, email address and whether the email domain matches the organisation that the sender claims to be from; • check the link before you click; • keep an eye out for spelling and grammatical mistakes; • be wary of third-party sources providing information regarding the Covid-19-coronavirus and refer to the official websites; • protect your devices with anti-spam, anti-spyware and anti-virus software and make sure they are always up to date; • visit websites directly by typing the domain name yourself. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>ENISA recommends that victims of a phishing attack should:</p> <ul style="list-style-type: none"> • update computer security software and run a scan; • change login credentials immediately; • contact bank/credit card company if bank details have been disclosed; • report a phishing email to the IT department by forwarding it as an attachment; • delete the email; and • notify any organisation being spoofed in order to prevent other people from being victimised. 		
EU	EU Agency for Cybersecurity (ENISA)	4/5/20	<p>ENISA publishes guidance on Computer Security Incident Response Teams (CSIRT) and their relevance during the Covid-19 coronavirus crisis</p> <p>The guidance highlights the relevance of CSIRTs to large companies, SMEs, private citizens, governments, and research and education institutions, particularly as many during the crisis look to the internet for their working models and are therefore more exposed to cybersecurity risk.</p>	<p>The guidance is available here.</p> <p>The map is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The guidance describes the nature of CSIRTs (front line response teams for cybersecurity incidents and attacks), provides a map of the same and flags the existence of the CSIRT Network (established by the NIS Directive). The CSIRT Network is intended to enable coordinated responses and exchanges cybersecurity information to enable swift action.</p> <p>The guidance also draws attention to training and materials available should an organisation want to set up an incident response team.</p>		
EU	EU Agency for Cybersecurity (ENISA)	27/4/20	<p>ENISA publishes advice to SMEs when choosing online communication tools in the context of the Covid-19 coronavirus outbreak</p> <p>ENISA provided some practical advice to SMEs with regard to the security and privacy aspects that should be considered upon the selection and use of online communication tools, including:</p> <ul style="list-style-type: none"> • make sure that the tool supports encrypted communication; • choose a tool that supports centralised management (such as call restriction and password policy); 	The advice is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • assess the security settings (including support for multi-factor authentication); • review configuration options; • read the privacy policy carefully (including regarding nature and location of data storage, data sharing) and consult your DPO; • use available work (rather than personal) resources and devices; • ensure use of latest, patched and up to date software; • password protect meetings; • verify default settings, record meetings only when necessary and obtain agreement to the same; and • take care when using video link and sharing materials or background to speaker. 		
EU	EU Agency for Cybersecurity (ENISA)	24/3/20	<p>ENISA publishes recommendations for teleworking and warns against phishing scams related to Covid-19</p> <p>ENISA published a brief guidance with recommendations on maintaining adequate level of</p>	The press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>cybersecurity for employers and employees on remote working in the context of Covid-19 coronavirus.</p> <p>The recommendations for employers mirror the guidance issued on 15 March 2020 and include, amongst other things:</p> <ul style="list-style-type: none"> • corporate VPN solutions should be scalable and capable to maintain multiple connections; • secure video conferencing for corporate clients; • encrypted communication channels should be used for accessing all business applications, access to the application portals should be safeguarded by MFA mechanisms, and mutual authentication is recommended when accessing corporate systems (e.g. client to server and server to client); • direct internet exposure of remote system access interfaces (e.g. RDP) should be prevented; • if possible, staff should be provided with corporate computers and devices with up-to- 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>date security software and security patch levels;</p> <ul style="list-style-type: none"> • BYOD must be vetted from the security standpoint using NAC, NAP platforms (e.g. patch check, configuration check, AV check etc.). • ensure adequate IT support resources for resolving technical issues of teleworking; • remind personnel about incident response and personal data breach policies; • processing of employee data in the context of teleworking (e.g. time keeping) should be compliant with data protection law. <p>Employees are recommended to, amongst others, when teleworking:</p> <ul style="list-style-type: none"> • where possible, use corporate rather than personal devices, ensure devices have updated operating system, software and antivirus and malware protection; make sure not to use same devices for leisure activities; • use secure networks for connecting to internet and check security of their home Wi-Fi 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>systems and avoid the exchange of sensitive corporate information through possibly insecure connections;</p> <ul style="list-style-type: none"> • never share the virtual meeting URLs on social media or other public channels to prevent unauthorised third parties from accessing closed meetings; • use corporate intranet resources for sharing working files and avoid sharing sensitive information across local devices; • be particularly vigilant with e-mails referencing the Covid-19 coronavirus; • encrypt data at rest, such as local drives, to minimise damage in case of theft or loss of the devices. <p>ENISA also issued a warning against growing number of phishing attacks exploiting the Covid-19 coronavirus pandemic. ENISA recommends utmost care when emails, even when coming from a trusted source, asking to check or renew login credentials, or include attachments hyperlinks. Emails that create a feeling of urgency or severe consequences or emails from contacts asking for unusual things should be</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			verified before any links are clicked or attachments are opened.		
EU	EU Agency for Cybersecurity (ENISA)	15/3/20	<p>ENISA issues a brief note on remote working</p> <p>ENISA published a brief note with recommendations for employers on remote working in the context of Covid-19 coronavirus.</p> <p>Amongst other things, it is recommended that employers:</p> <ul style="list-style-type: none"> • provide authentication and secure session capabilities such as encryption; • prioritise support of remote access solutions; • provide virtual solutions such as electronic signatures; • define a security incident procedure and educate staff on reporting and emergency processes; • consider restricting access to sensitive systems. <p>The note also highlights the increased risk of phishing attacks and what to look out for.</p>	The note is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
EU	European Union Agency for Fundamental Rights (EU FRA)	7/4/20	<p>The European Union Agency for Fundamental Rights announces a report on the implications of Covid-19 coronavirus on human rights, including privacy and data protection</p> <p>The EU FRA has published a report on the Covid-19 coronavirus pandemic and its implications for human rights, including data privacy.</p> <p>Section 4.2 in particular flags that data protection goes hand in hand with rights to health and that data protection concerns are not hindering the fight against the Covid-19 coronavirus. It also describes the potential for data protection concerns arising in the context of employer processing of health and travel data, the production of DPA guidance and the lack of harmonisation across EU member states e.g. in relation to disclosure of names of infected employees.</p>	<p>The press release is available here.</p> <p>The report is available here.</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Austria	Austrian supervisory authority (DSB)	27/3/20	<p>DSB updates its guidance on processing personal data in relation to the Covid-19 coronavirus, security of remote work guidance, FAQs and a model form for collecting personal details of employees</p> <p>The DSB updated its page dedicated to guidance on Covid-19 coronavirus and processing of personal data and related documents.</p> <p>In particular, the DSB clarified the following:</p> <ul style="list-style-type: none"> • data protection law allows processing of health data of individuals to the extent necessary to curb the spread of the virus and to protect others. In the context of labour law, the specific legal basis for data processing is Article 9(2)(h) General Data Protection Regulation 2016 (GDPR) (processing for the purpose of healthcare) and Article 9(2)(b) GDPR (processing for the purpose of fulfilling labour and social law obligations). Transfer of health data of employees to the health authorities can be done on basis of Art. 9(2)(i) GDPR (processing for public interest reasons 	<p>The guidance is available here.</p> <p>The FAQs are available here.</p> <p>The security of remote work guidance is available here.</p> <p>The model form is available here.</p> <p>(all only in German)</p>	<p>Cybersecurity and information security</p> <p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>in the field of public health) and in accordance with Section 5 (3) of the Epidemic Act 1950;</p> <ul style="list-style-type: none"> employers may request (but not require) and temporarily store the employees' private mobile phone number in order to be able to warn them at short notice about an infection within the organisation. The DSB provided a model form for collection of personal contact details of employees; employers may not use health data of employees for purposes other than healthcare, containment of the virus and treatment, and must delete data after the end of the epidemic. <p>In relation to the increased use of home workspace, employers should specifically inform employees about security requirements in relation to hardware (such as service laptops and company phones) and the use of secure Wi-Fi connection, strong password policy and increased risks due to phishing attacks abusing the issue of Covid-19 coronavirus.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Belgium	Belgian DPA	2/4/20	<p>Belgian DPA updates guidance on Covid-19 coronavirus and data processing in employment context</p> <p>The Belgian DPA updated its guidance and FAQs on the processing of personal data in the workplace in relation to Covid-19 coronavirus, which was initially published on 13 March 2020. The guidance is intended to help employers reconcile their obligations to provide a safe and healthy working environment for their employees with an obligation of employers to protect the employees' right to privacy and protection of personal data. The Belgian DPA referred to the preventive measures that employers are required to take to contain the infection in their organisations, as published by the Federal Public Service for Employment, Labour and Social Dialogue (the FPS) (available here in Dutch and here in French, and updated guidance here in Dutch). These measures include, for instance, organisation of flexible working hours, teleworking, deferral of social events for employees, as well as raising awareness about hygiene and social distancing.</p> <p>The Belgian DPA highlighted that if these preventive measures involve processing of personal data,</p>	<p>The guidance is available here (in French) and here (in Dutch).</p> <p>A note by the DPA about limited availability due to Covid-19 coronavirus measures is available here (only in Dutch).</p>	<p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>employers should respect requirements of the GDPR and continue to follow the general principles of proportionality and data minimisation in relation to workplace processing activities, be transparent about the collection and retention of personal data, and implement appropriate security measures to protect personal data.</p> <p>The Belgian DPA also noted that:</p> <ul style="list-style-type: none"> • any processing of personal data must comply with the conditions of Article 6(1) GDPR and must be based on one of the legality grounds stated in this Article, also in the context of taking preventive health measures during the pandemic; • at the current stage of the pandemic and on the basis of the latest information published by the FPS on Covid-19, processing in the context of taking preventive measures by companies and employers cannot be broadly or systematically based on the legitimacy ground contained in Article 6(1)(d) GDPR (processing is necessary in order to protect the vital interests of the data subject or 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>another natural person), and even less so for the processing of health data of employees that are special categories of data;</p> <ul style="list-style-type: none"> • for the processing of health data employers can only rely on article 9(2)(i) GDPR (processing is necessary for reasons of public interest in the area of public health on basis of the EU or member state law) when they act in accordance with explicit guidelines imposed by the competent authorities; • health risk assessments should be carried out not by employers but by the occupational physician competent to detect infections and inform the employer and the persons who came into contact with the infected person. This information can be provided by the company doctor on the basis of Art.6(1)(c) and 9(2)(b) GDPR (processing necessary for compliance with an employment legal obligation); • the Belgian DPA has changed its position on monitoring body temperature of employees, stating that it does not consider mere checks 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of body temperature as personal data processing. Insofar as such temperature checks do not involve additional registration or processing of personal data, the GDPR does not apply. However, the Belgian DPA notes that in this case employers cannot take measures that go beyond the existing employment law regulatory framework or instructions from competent authorities;</p> <ul style="list-style-type: none"> • employers cannot oblige workers to fill in health questionnaires or questionnaires about recent travel; however, employers may encourage employees to disclose such information voluntarily and refer them to the occupational physician if appropriate; and • the name of individuals who have contracted Covid-19 coronavirus cannot be revealed to co-workers, however, the information about contracted infection can be revealed without naming individuals. The name of the infected person may, however, be communicated to the occupational physician or the competent government services. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Belgium	Belgian DPA	1/4/20	<p>Belgian DPA issues brief guidance on Covid-19 coronavirus and health apps</p> <p>The Belgian DPA published brief guidance on the use of various data in the fight against the Covid-19 coronavirus epidemic.</p> <p>The Belgian DPA notes receiving numerous questions on this topic and observing an increasing number of apps on the market that do not appear to comply with data protection law. Its recommendations include:</p> <ul style="list-style-type: none"> • processing anonymous data: unless necessary, the app should not collect and process personal data of patients. The Belgian DPA reiterates that personal data are defined broadly and include directly identifying data (such as name, email address, national identification number, mobile phone number etc.) or other data (e.g. ID of the device or of the connection) that in combination with other data allows a patient to be indirectly identified. The guidance clarifies that that data is only then anonymous when it can no longer lead to re-identification of an individual in combination with other data, including third party data (noting that IP 	The guidance is available here (in French) and here (in Dutch).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>addresses are always personal data, because re-identification of a person is always possible with assistance of a telecom operator);</p> <ul style="list-style-type: none"> • if an app as part of an existing healthcare relationship between a patient and a healthcare provider or healthcare institution, this should be explicitly stated by the healthcare provider. Personal data should only be processed through the app by that healthcare provider in the context of the quality and continuity of services. It is preferable that a patient is invited by the healthcare provider to use the app; • in any other cases, an app that involves processing of personal data must provide on the very first screen, and before the users enter any personal data or any of their personal data are collected, the information required by the GDPR (including the controller identity, the precise purposes of the processing, whether the cookies are used etc.). The patient should not be required to provide any directly identifying personal data when starting the app. The app can only use 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>personal data that are necessary for the proper functioning of the app for the stated purposes and under the responsibility of the identified controller. When users stop using the app, they should be given a choice to transfer personal data to that healthcare provider (e.g. passing on the results of self-evaluation to a family doctor) or to a different healthcare provider. In such a case, the patient may be asked to provide additional personal data and all such data can be transferred to the healthcare provider, otherwise all personal data of the app user must be deleted and cannot be used for other purposes.</p>		
Croatia	Personal Data Protection Agency (AZOP)	18/3/20	<p>AZOP issues statement on employee data and the Covid-19 coronavirus pandemic</p> <p>AZOP confirmed that any collection and processing of personal data must be in accordance with the GDPR, requires a lawful basis under Article 6(1) and, in relation to health data, an exception to the processing prohibition under Article 9(2). The guidance also notes that any data processing must be in accordance</p>	The statement can be found here (available only in Croatian).	Data processing-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>with the general principles outlined in Article 5, such as proportionality and necessity.</p> <p>In relation to the lawful basis for processing employee personal data, AZOP commented that an employer could rely upon its legal obligations, or the protection of the vital interests of data subjects or other natural persons (Article 6(1)(c) and (d) GDPR).</p>		
<p>Czech Republic</p>	<p>Office for Personal Data Protection (UOOU)</p>	<p>22/4/20</p>	<p>UOOU publishes an updated FAQ document on the conditions that the Ministry of Health and healthcare providers have to meet in relation to informing of the public about the Covid-19 coronavirus patients and victims.</p> <p>According to the UOOU, the personal data about the patients disclosed to the public must be anonymised, while all means leading to indirect identification of the individuals should be taken into consideration.</p> <p>In particular, the Ministry and healthcare providers should not disclose information about the residence of the patients, especially if they are residing in small towns.</p> <p>Lastly, the UOOU highlights that personal data protection does not apply to the data of deceased persons, and that the publication of anonymised data</p>	<p>The press release is available here.</p> <p>The FAQs are available here.</p> <p>(both in Czech only)</p>	<p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			of deceased persons does not interfere with the privacy of their family, as it does not lead to identification of the family members.		
Czech Republic	Office for Personal Data Protection (UOOU)	2/4/20	<p>UOOU publishes statement on emergency measure to process location data by telecoms operators and banks during Covid-19 coronavirus pandemic</p> <p>The UOOU issued a statement about emergency measures of the Ministry of Health ordering mobile communication network operators and banks to trace the movement and behaviour of individuals infected with Covid-19 by processing the time and location data of the use of electronic means of payment. In particular, the UOOU highlighted that the processing of personal data for the purpose of combating a pandemic or preventing the deterioration of a pandemic must be adequate, effective, and limited in time.</p> <p>The emergency measure stipulates that controllers will act at the request of state authorities and within the limits of the measure. The UOOU noted that the legal obligations imposed in connection with the fulfilment of an emergency measure by the Ministry of Health and regional hygiene offices for data</p>	The press release is available here (only in Czech).	Data processing- location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>processing by controllers, such as banks, should be for the fulfilment of a task performed in the public interest, as provided under Art, 6(1)(e) GDPR.</p> <p>However, the UOOU outlined that it is up to each controller (including each bank or telecoms operator) to determine and undertake the required processing of behavioural data defined in the order of the Ministry or the regional hygiene office. Furthermore, the UOOU stressed that an emergency measure provides for the retention of personal data only for as long as it is necessary and, in case of non-anonymised data, not longer than six hours. The data must then be erased or fully anonymised to prevent misuse for purposes other than the fight against the Covid-19 coronavirus.</p>		
<p>Czech Republic</p>	<p>Office for Personal Data Protection (UOOU)</p>	<p>20/3/20</p>	<p>UOOU issues guidance on Covid-19 coronavirus and data processing</p> <p>The UOOU issued a frequently asked questions (FAQs) document regarding data protection in the context of the Covid-19 coronavirus. Amongst others, the FAQs clarify the following key points:</p> <ul style="list-style-type: none"> • contact details of members of local Covid-19 coronavirus task forces operating in 	<p>The press release is available here.</p> <p>The FAQs are available here. (both in Czech only)</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-location data</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>municipalities can be stored on servers located abroad;</p> <ul style="list-style-type: none"> the Covid-19 coronavirus epidemic is considered an emergency under Article 9(2)(a) of the GDPR and competent authorities for the protection of public health are thus authorised to undertake epidemiological investigations and request relevant information from individuals; during the current emergency state, telecommunications operators may trace the movement of infected people based on location data from their mobile phones subject to adhering to general principles governing processing of personal data; health information about an employee infected by the Covid-19 coronavirus can only be processed and disclosed by the employer when this is necessary for protection of health of the other employees. 		<p>Data processing- public authorities</p> <p>Data processing- health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Denmark	Danish Datatilsynet	17/4/20	<p>Danish Datatilsynet publishes statement on Covid-19 tracking app</p> <p>The statement explains that a Covid-19 tracking app is under development in Denmark. The app will track possible contacts of those infected with Covid-19, and the statement notes that this presents potential privacy intrusions.</p> <p>Accordingly, the statement highlights that controllers must focus on the necessary balance between the need to find a solution to the Covid-19 pandemic and the rights of individuals, especially with respect to transparency. It also stresses the importance of carrying out data protection impact assessments prior to any processing where that processing presents high risks to individuals' rights. Key factors the DPA should consider in relation to apps include:</p> <ul style="list-style-type: none"> • voluntary nature; • minimum data processing necessary; • transparency-clear who is behind the app and what happens to information; • security of collection and storage of information; 	The statement is available here (only in Danish).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> Temporary solution. 		
Denmark	Danish Datatilsynet	16/3/20	<p>Danish Datatilsynet publishes data protection recommendations for home working</p> <p>The Danish Datatilsynet issued its recommendations to organisations and employees on data protection issues related to remote working triggers by Covid-19 coronavirus measures. The recommendations include:</p> <ul style="list-style-type: none"> establishing clear guidelines for homeworking and making sure employees follow these guidelines; using designated secure access to company systems (e.g. VPN or direct connection); to the extent possible, using the normal central data management systems, where access control, document version control, backup and general security are in place; any hardcopies of documents with information about natural persons should be stored and disposed of in secure manner; if there is an urgent need to store documents containing sensitive personal data on local 	The recommendations are available here (only in Danish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>devices, the device or file with the document must be encrypted, no third persons (including children) should have access to this device, the file should be uploaded to the document management system as soon as possible and the local copy deleted immediately.</p> <p>The Danish Datatilsynet further referred to the guidance issued by the Center for Cyber Security on 15 March 2020.</p>		
Denmark	Danish Datatilsynet	12/3/20	<p>Danish Datatilsynet announces its limited availability due to Covid-19 coronavirus and expressed an understanding that compliance deadlines may be missed</p> <p>The Danish Datatilsynet issued a press release in relation noting its limited availability due to government requirements to avoid working in the premises due to the Covid-19 coronavirus pandemic.</p> <p>The Danish Datatilsynet clarified that it will show understanding to companies, authorities and organisations that may have difficulty in complying with the response deadlines, injunctions and other orders given by the supervisory authority. In these</p>	The press release is available here (only in Danish).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			cases, the Danish Datatilsynet urges such entities to contact the authority to make further arrangements.		
Denmark	Danish Datatilsynet	5/3/20	<p>Danish Datatilsynet issues guidance for employers on data processing and Covid-19 coronavirus</p> <p>The Danish Datatilsynet issued a press release on the implications of GDPR and the Covid-19 coronavirus. The authority stated that employers could record and disclose non-specific data as this would likely not amount to health data under the GDPR, for example, if an employee returned from a risk area, or if they were quarantined or unwell (without specifying the reason).</p> <p>Under certain circumstances, the employer may also record and disclose health data, for example, in order for management to take necessary precautions. The Danish Datatilsynet reiterated that recording and sharing such information is subject to a necessity and proportionality test. Employers should consider whether the same purpose can be achieved through less information or without naming the person.</p>	The press release is available here .	Data processing- employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Denmark	Centre for Cybersecurity (CCS)	24/4/20	<p>CCS publishes recommendations on cybersecurity practices for return to work</p> <p>The CCS recommendations on cybersecurity when returning to the workplace following the Covid-19 pandemic (the Recommendations) explain that IT and security managers must prepare and effectively communicate what is expected of employees upon their return to the workplace.</p> <p>In particular, the Recommendations provide high level guidance to employees including:</p> <ul style="list-style-type: none"> • ask IT support about how the IT equipment that has been with you at home or is shared can be cleaned; • transfer all work-related files saved locally to, for example, common drive from which backup is performed; • remove any personally identifiable data or other sensitive data from the IT equipment you have used (ensure correct procedure followed for effective deletion); • hand over the extra IT equipment that has been borrowed during homework. Be aware of 	<p>The press release is available here.</p> <p>The Recommendations are available here. (both only in Danish)</p>	<p>Cybersecurity and information security</p> <p>Returning to the workplace</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>private information on the including usernames and passwords stored in the browsers;</p> <ul style="list-style-type: none"> • uninstall the programs on the equipment that the workplace has not normally approved for use and which have been required to install during the homework period. <p>With respect to employers, the Recommendations:</p> <ul style="list-style-type: none"> • set out that IT managers must review IT accounts, communication links, access rights and IT solutions that have been implemented as emergency measures, in order to revoke them when the emergency is over; • suggest consideration of contingency and crisis management plans to assist in transition; • highlight the importance of thorough reviews of logs in order to confirm whether an incident has occurred; • suggest rectifying operating conditions that have not been managed fully during the crisis e.g. scheduled service maintenance; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • suggest that a complete review of personal computers should be undertaken with an updated virus tool upon employees' return to the workplace; • suggest strengthening service desk for short period; and • suggest reviewing best practice for future reference. 		
Denmark	Centre for Cyber Security (CCS)	8/4/20	<p>CCS issues a statement on system vulnerabilities caused by increased use of remote access stemming from Covid-19 coronavirus</p> <p>The CCS highlighted in its statement several instances in which VPN gateway vulnerabilities have been exploited to compromise networks with, amongst other things, ransomware.</p> <p>The CCS also noted that for industrial control systems, it is particularly important to ensure that access is protected, as an increase in the number of exposed control systems has been observed due to the increased need for employees to work from home.</p> <p>Finally, the CCS outlined that another tool for remote access is remote desktop protocol which, amongst</p>	The press release is available here (only in Danish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			other things, should be protected by two-factor authentication.		
Denmark	Center for Cyber Security (CCS)	1/4/20	<p>Center for Cyber Security issued five cybersecurity advisories for individuals to address malicious actions related to Covid-19 coronavirus</p> <p>The CCS published advice for individuals to improve their cybersecurity awareness and help recognise malicious actors abusing the Covid-19 coronavirus pandemic, including fake domains similar to domains of official healthcare institutions on the pandemic that disseminate malware and are used for phishing attacks.</p>	<p>The press release is available here (only in Danish).</p> <p>The page with five advisories is available here (only in Danish).</p>	Cybersecurity and information security
Denmark	Center for Cyber Security (CCS)	31/3/20	<p>Center for Cyber Security publishes guidance on security of communication and collaboration platforms used for homeworking during Covid-19 coronavirus pandemic</p> <p>The CCS published new guidance on the secure use of platforms that facilitate communication and collaboration between employees and teams such as Skype, Slack, WeTransfer, Dropbox, Microsoft Teams, WhatsApp, Starleaf and other similar platforms. The guidance clarifies how these platforms can be used safely. The recommendations include:</p>	<p>The press release is available here and the guidance here (both only in Danish).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • perform a prior risk assessment of the use of communication and collaboration platforms, particularly if those will be used to process valuable or sensitive information; • review the platform user terms and conditions (EULA), which might stipulate the use of data mining applied by the provider to user information and data shared via platforms; • confirm that communication and data shared via the platform are encrypted and carefully consider what information may be processed through these services; • after the risk assessment is performed, clearly inform employees of the platforms that can be used for work-related collaboration and what internal rules apply to sharing information via these platforms; • in any event, consider using internationally recognised collaboration platforms from major suppliers that undergo regular security evaluations and reviews. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Denmark	Center for Cyber Security (CCS)	27/3/20	<p>Center for Cyber Security publishes guidance on protecting RDP access</p> <p>The CCS published guidance for organisations on how to protect themselves against hackers targeting remote desktop protocol access (RDP). The CCS notes that where RDP access is not protected by, for instance, a VPN or multi-factor authentication, the RDP may be easily compromised, especially by malware designed specifically to attack RDP access.</p> <p>The guidance encourages IT security officers to:</p> <ul style="list-style-type: none"> • implement VPN access; • require two-factor authentication before accessing an organisation's IT systems; • ensure the RDP access mechanism is up to date; • validate access with strong passwords (noting the CCS's guide to choosing and maintaining strong passwords); and • close all redundant employee accounts. 	<p>The guidance is available here (only in Danish).</p> <p>The CCS password guide is available here (only in Danish).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Denmark	Center for Cyber Security (CCS)	15/3/20	<p>CCS issues a threat assessment for the use of home workplaces in light of Covid-19 coronavirus</p> <p>The CCS published a threat assessment of remote working and using home workplace in light of the Covid-19 coronavirus pandemic. The new threat assessment indicates very high levels of cyber risks faced by organisations due to the increased use of home workplaces that normally have lower levels of safety and security than workplaces within organisations and corporate networks.</p> <p>The CCS urges companies to scale up their efforts and take necessary measures for protecting home workplaces and their networks from cyber threats. The press release clarifies that although maintaining the usual IT security levels with timely updates, two-factor authentication and VPN can be difficult, the Covid-19 Coronavirus crisis represents a particularly favourable opportunity for cyber criminals to attack networks. This means that weakening security measures in favour of the usability should only be done after a thorough risk assessment of the possible consequences.</p> <p>The threat assessment lists recent examples of malware attacks using fake Covid-19 Coronavirus</p>	<p>The press release is available here.</p> <p>The threat assessment is available here.</p> <p>The list with tips is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>websites and phishing emails claiming to represent health authorities.</p> <p>The CSS further issued a list with practical tips for organisations and employees to ensure security of remote working from home.</p>		
Estonia	Data Protection Inspectorate (AKI)	20/3/20	<p>AKI produces further guidance on the processing of employee data in the context of Covid-19 coronavirus</p> <p>The AKI published detailed guidance on the processing of personal data in the employment context in relation to the Covid-19 coronavirus pandemic. This guidance follows the AKI's initial statement on the legal basis for processing such data and reiterates the advice to employees that they should co-operate with their employer and consider disclosing matters relating to their health where this would reduce the spread of communicable diseases. Employees must remember that they can only start work if they are healthy and that their employer is entitled to confirm this (but does not need to know the exact diagnosis).</p> <p>The guidance also provides advice to employers. Specifically, employers should ensure the safety of</p>	The guidance is available here (only in Estonian).	<p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the working environment and evaluate how its usual processes may no longer be appropriate in an emergency. Employers may ask whether their employee has been in a risk area or exposed to affected people, but it is preferable for information on symptoms to be exchanged by mutual understanding between employer and employee.</p> <p>AKI further provides a detailed analysis of various bases for processing personal data that can be considered for in this context. The guidance also sets out the specific provisions of Estonian and EU law that are particularly relevant to the Covid-19 coronavirus pandemic, including legislation beyond data protection laws, such as emergency laws adopted to tackle the pandemic.</p> <p>In addition, the AKI further confirmed that informing other employees that one employee is suffering from an infectious disease in a way that identifies that employee is only permitted if such information is communicated to other employees in order to protect their life, health or liberty, and consent cannot be obtained from the employee concerned. The same is true for individuals from other organisations that the employee may have come into contact with, such as</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			at a meeting. An infectious disease that a worker could acquire from anywhere is not sufficient justification to disseminate health data.		
Estonia	Data Protection Inspectorate (AKI)	16/3/20	<p>AKI addresses processing of employee data in the context of Covid-19 coronavirus</p> <p>The AKI published a statement in relation to the Covid-19 coronavirus pandemic and employers' rights to request employee medical records. The statement confirms that, as health data cannot be processed on the basis of legitimate interest, the individual's valid consent may be required as lawful basis.</p> <p>However, the AKI also encourages employees to voluntarily provide their employer with health information in the interests of public health in order to allow the employer to protect other employees and workplace.</p>	The statement is available here (only in Estonian).	Data processing-employment Data processing-health status
France [Updated as at 21 May 2020]	French supervisory authority (CNIL)	20/5/20	<p>CNIL adopts guidance on monitoring online exams during the Covid-19 coronavirus crisis.</p> <p>The CNIL Guidance addresses privacy issues arising when an educational establishment conducts remote exams.</p>	<p>The Guidance is available here.</p> <p>Remote education plan of 15 April is available here.</p>	Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>It confirms, amongst other things, the need to comply with the GDPR to avoid infringing the privacy of individuals being filmed and makes suggestions to avoid infringing the privacy of others that may be in the room.</p> <p>The guidance advises on the likely legal bases for processing (for example performance of a task of public interest; not consent due to student/institution relationship).</p> <p>It also highlights the need to account of the principles of proportionality, data minimisation, and processing purpose. The CNIL notes by way of example that it does not consider processing activities such as video surveillance for the exam's duration, the taking photographs or recording sounds to be disproportionate. However, use of facial recognition and monitoring devices to check a student's access to email and social networks, would be considered disproportionate in this context.</p> <p>The guidance includes recommendations regarding issues such as data retention, data storage, data security, encryption, data access rights, and it also specifies that a DPIA must be conducted particularly if</p>	<p>(Both only available in French)</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>innovative technologies, such as eye tracking, are used.</p> <p>Finally, the guidance provides some advice for students, including regarding their rights as data subjects.</p> <p>This guidance is relevant to the plan issued by the Ministry of Education on 15 April regarding distance education and solutions for remotely monitoring written exams.</p>		
France	Conseil D'Etat	18/5/20	<p>Conseil D'Etat issues decision ordering French state to stop using drones to monitor lockdown</p> <p>The Conseil D'Etat has issued a decision ordering that the practice of capturing images by drone and using these to enforce the Covid-19 coronavirus lockdown in Paris should be stopped until required authorisations have been obtained under French law or technical changes are made to prevent identification of persons filmed.</p> <p>The Conseil D'Etat ruled on a claim from the organisations "La Quadrature du Net" and the League for Human Rights that the right to privacy should not be conditional on the device used to process the personal data. The claim further stated that the use of</p>	<p>The decision can be found here.</p> <p>The announcement from the French supervisory authority can be found here. (Both only in French).</p>	<p>Data processing – public authorities</p> <p>Mobile apps and new technology</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>drones in this way violates the GDPR and EU human rights law in many respects, for example no fair processing information is provided to individuals and there is no set data retention period.</p> <p>In response, representatives of the state argued that the use of the surveillance measures was legitimate and only intended to directly enforce health security rules. The Conseil D'Etat did consider this a legitimate purpose and did note that drone instructions specified real-time filming should occur at heights such that individuals could not be identified. However, it ultimately ruled in favour of "La Quadrature du Net" and the League of Human Rights. The drones had the ability to zoom in, fly at lower heights and identify natural persons. They were not equipped with technical methods to prevent use for purposes beyond the intended general area assessment and which would involve the processing of personal data of the sort which requires prior approval and account of the opinion of the CNIL. Given the risks of use contrary to data protection law, the processing of personal data without authorisation is regarded as an illegal infringement of the right to respect for private life.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The CNIL has been investigating and will continue to investigate the use of drones in France more widely, is waiting on further response from the Interior Ministry and will take a position on the issue in due course.		
France	French supervisory authority (CNIL)	14/5/20	<p>CNIL reports on its opinion regarding the draft decree for information systems to monitor Covid-19 coronavirus patients</p> <p>On 8 May, the CNIL issued an opinion regarding a draft decree setting out the terms and conditions of use of two information systems for monitoring patients (named "SI-DEP" and "Contact Covid"). As further described in the overview below, the decree is associated with a law extending the state of health emergency in France that, amongst other things, addresses information systems for collection of personal data to assist in the fight against the Covid-19 coronavirus crisis.</p> <p>On 14 May, the CNIL comments on its opinion and notes the approach taken in the final published decree Décret n° 2020-551 du 12 mai 2020 and the associated law LOI n° 2020-546 du 11 mai 2020.</p> <p>The information systems "SI-DEP" and "Contact Covid" addressed in the decree are intended to</p>	<p>The opinion is available here.</p> <p>The press release from the CNIL is available here.</p> <p>The final decree itself is available here (only in French).</p> <p>The final law itself is available here (only in French).</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>identify those who have been infected and those who are at risk of infection, providing medical referrals where necessary, and to assist with research into the pandemic and surveillance on a national scale. The CNIL considers that the measures proposed generally comply with the GDPR. It notes that, in light of the scientific analyses gathered by the French Government, the planned system of health investigations and epidemiological monitoring is necessary for the lockdown exit but stresses that the invasion of privacy by these processing activities is only justified if the policy is the appropriate response to slow the spread of the pandemic.</p> <p>The CNIL opinion of 8 May set out that this processing of personal data should be reassessed periodically, to confirm that it is still necessary to control the pandemic. The CNIL also emphasised that the permitted purposes for the processing must be interpreted narrowly and that only strictly necessary categories of data should be collected and processed.</p> <p>While the CNIL considered that the approach to the information systems in the draft decree was generally GDPR-compliant, it requested clarification of certain issues. These requested clarifications have been</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>addressed in the final Décret n° 2020-551 du 12 mai 2020 and the associated law LOI n° 2020-546 du 11 mai 2020, including, amongst others:</p> <ul style="list-style-type: none"> • a more precise framework for the data to which each database user will have access; • avoiding collection of information regarding the connection between a patient and contact (the final decree provides for collection of a category of connection only, ie, whether the contact is known, cohabits, date of last contact); • further reflection on data retention (LOI n° 2020-546 du 11 mai 2020-limits data retention to 3 months from date of collection); • the need for relevant staff using the systems to be trained and for a traceability system to be implemented such that any abuse can be detected and punished. <p>The CNIL also noted that the draft decree effectively ruled out the right to object to data processing, only allowing the "patient 0" to stop his name being revealed to his "contact cases" and to stop certain transmissions of his data for research purposes. The</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>CNIL asked that the restriction on the right to object be reduced to a minimum and notes that in the final Décret n° 2020-551 du 12 mai a right to object has been included for "case contacts" regarding the processing of their data in Contact Covid. The rights to be informed, the right of access and the right to rectification will also be guaranteed.</p> <p>The CNIL considers that the final Décret n° 2020-551 du 12 mai accounts for the CNIL's main requests and notes that certain other recommendations will follow the implementation of the system (such as security measures regarding password authentication or traceability of certain actions).</p> <p>The CNIL will continue to closely monitor the system and inspect in the few weeks following implementation.</p>		
France	French supervisory authority (CNIL)	12/5/20	<p>CNIL publishes guidance for employees on the protection of personal data in remote working</p> <p>The CNIL has published a set of practical actions that it advises employees to take where their employer has adopted teleworking practices due to the Covid-19 coronavirus pandemic. The guidance emphasises that</p>	The guidance is available here (only in French).	Data processing - employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>its aim is to guarantee the safety of the employees and of their company.</p> <p>The steps that the CNIL recommends for employees include:</p> <ul style="list-style-type: none"> • following the employer's instructions, including any charter for teleworking; • securing their internet connection, such as by placing a complex password on their Wi-Fi network; • using any VPN provided by their company as much as possible; • making sure that any personal computer used is secured (including through the use of antivirus software and firewalls, a personal account and regular back-ups); • ensuring the security of any personal phone used for work (such as by only installing apps from known sources and avoiding PIN codes that are too obvious); • prioritising the security of communications, through the use of authorised applications and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>videoconferencing systems that promote an expectation of privacy; and</p> <ul style="list-style-type: none"> • being particularly vigilant of any phishing attempts. 		
France	Constitutional Council of France (the Constitutional Council)	11/5/20	<p>Constitutional Council issues decision criticising aspects of the draft law extending the state of emergency in France and these concerns are addressed in the published law of 12 May 2020</p> <p>On 9 May a draft law was introduced in France to extend the state of emergency prompted by the Covid-19 coronavirus pandemic. The draft law addressed, amongst other things, the use of information systems to collect personal data without reliance on data subject consent; detail of to the purposes for which the information systems were used (including contact tracing); and the organisations that have access to the systems.</p> <p>The Constitutional Council validated several of its provisions but expressed its disapproval of the law's treatment of the processing of personal data relating to an individual's health for contract tracing purposes.</p> <p>In particular, the Constitutional Council criticises the provision that personal data relating to the health of people affected by Covid-19 coronavirus (and those</p>	<p>The decision is available here.</p> <p>The Council's press release is available here.</p> <p>(All only in French).</p>	Data processing – health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>close to them) may be processed without that individual's consent. The decision also emphasises that this processing will occur on a particular large scale, due to the information required to fight the pandemic. The Constitutional Council suggests steps that can be taken to limit the impact on privacy, such as limiting the system of information collection in time to that strictly necessary to combat the pandemic (or six months from the end of the state of emergency).</p> <p>The Constitutional Council also sets out the requirements for the contact tracing measures to comply with privacy principles on a more general basis, such as that the measures taken must be appropriate, necessary and proportionate to the relevant risks.</p> <p>The reservations and censures expressed by the Constitutional Council in its decision of 11 May have been subsequently addressed in Articles 11 and 13 of the draft bill before its official publication as the LOI n° 2020-546 du 11 mai 2020 on 12 May 2020.</p> <p>The LOI n° 2020-546 du 11 mai 2020 permits collection of personal data for the purposes of contact tracing without reliance on data subject consent but only for a period of 6 months from end of state of</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>emergency. Any data collected may only be held for a period of 3 months. LOI n° 2020-546 du 11 mai 2020 amongst other things, continues to describe the purposes of the information systems and the organisations that have access to the same. It notes their requirement to keep the data confidential and comply with professional secrecy obligations and the existence of penalties for failure to do so. LOI n° 2020-546 du 11 mai 2020 also provides for audit of the systems to ensure compliance with, amongst other things, data protection requirements.</p> <p>An associated decree Décret n° 2020-551 du 12 mai 2020 also of 12 May 2020 provides more detail regarding data protection (for example, the data controllers, the categories of data processed, the rights of access to data, the recipients, as well as their retention period and the procedures for the exercise of GDPR data subject rights) with respect to two distinct processing operations, Contact Covid and SI-DEP. See above in this overview regarding the CNIL's opinion on the same.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French Labor Ministry (the Labor Ministry)	3/5/20	<p>Labor Ministry publishes a national protocol for exiting lockdown prompted by the Covid-19 coronavirus pandemic</p> <p>The Labor Ministry has released a document setting out the steps businesses in France should take to exit the national lockdown safely. In particular, the guidance aims to reduce the risk of exposure to Covid-19 coronavirus, help organisations assess risks that cannot be avoided and promote collective protection measures over individual protection measures.</p> <p>The protocol provides specific recommendations and worked examples in eight areas: physical distancing and barriers, maintaining open spaces, managing the flow of people, personal protective equipment, dealing with any people showing symptoms of the virus, taking temperatures and cleaning and disinfection.</p> <p>The Labor Ministry emphasises that the viral testing procedure is complex and must be carried out by medical professionals, so organisations cannot organise their own testing programmes. The protocol also provides a warning to exercise caution with temperature testing, as the Covid-19 coronavirus may be asymptomatic or any symptoms may not include a fever. A temperature control at the entrance of</p>	<p>The protocol is available here.</p> <p>The accompanying press release is available here.</p> <p>Both only in French).</p>	Data processing – health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>establishments is not recommended but rather it is recommended that individuals measure their own temperature and more generally monitor for symptoms.</p> <p>If temperatures screening is established by an organisation it must comply with the relevant labor law requirements, it must be proportionate to the objectives, automated temperature capture such as thermal cameras should not be used and mandatory temperature readings should not be recorded in an automated or paper system. The protocol confirms that temperature control is not recommended and employees are entitled to refuse the same.</p>		
France	French supervisory authority (CNIL)	7/5/20	<p>CNIL issues guidance for employers on collecting employee personal data when resuming commercial activity</p> <p>The CNIL has published guidance reminding individuals and professionals of the data protection principles that will apply to the lifting of any lockdown prompted by the Covid-19 coronavirus pandemic.</p> <p>In particular:</p> <ul style="list-style-type: none"> the CNIL reminds employers that they are responsible for the health and safety of their 	<p>The guidance is available here.</p> <p>The Q&As are available here. (Both only in French).</p>	Data processing - employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>employees, in accordance with the French Labor Code. The GDPR also permits employers to process personal data when strictly necessary to comply with their legal obligations;</p> <ul style="list-style-type: none"> the CNIL emphasises that employees and agents are responsible for preserving not only their own health but that of others they may come into contact with in the course of their work. For example, employees and agents must inform their employer if they have caught or suspect they have caught the virus (ie provide more health information that would normally be expected) unless they are working remotely or in isolation and therefore would not come into contact with colleagues or the public (in which case standard work procedures apply). It is therefore legitimate to remind employees of this obligation and to facilitate transmission (e.g. through a dedicated secure channel) amongst other things; and the CNIL notes that personal data processed by the employer must be strictly necessary for the fulfilment of legal and contractual obligations for example to take organisational measures (such as referral to the occupational doctor, telecommuting), 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>training and information and prevention of occupational risk. As such the employer can only deal with the elements linked to the date, the identity of the person, the fact that they indicated that they was contaminated or suspected of being contaminated, as well as the organisational measures taken. If necessary, the employer may communicate to certain health authorities those elements necessary for possible health or medical care of the exposed person. In any event, the identity of the person likely to be infected must not be communicated to other employees.</p> <ul style="list-style-type: none"> • the CNIL also reiterates the requirements for the processing of special category data, including health data, under the GDPR, noting likely legal bases (Art 9(2)(b), Art 9(2)(h)). • The CNIL provides specific guidance on the use of temperature checks at the entrance to premises and the completion of health questionnaires. The CNIL notes that employers themselves should not establish body temperature records for example, nor install automatic temperature sensing tools such as imaging cameras. Only manual temperature checks without contact, recording or 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>other action may fall outside the scope of GDPR requirements.</p> <ul style="list-style-type: none">• Further, the CNIL reminds employers that screening campaigns organised by employers are not permitted (according to DG of Labor) and that only competent health personnel can collect, implement and access any medical files or questionnaires from employees containing health information amongst other things. The employer may only receive a fitness or inability to work status without further information.• The CNIL makes further comment on the need to maintain security and confidentiality of data processed as business continuity plans are implemented.• The guidance links to a Q&A website produced by the French Labor Ministry, which includes information on other issues presented by the Covid-19 coronavirus pandemic such as childcare issues and the wearing of masks.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French supervisory authority (CNIL)	1/5/20	<p>CNIL publishes guidance of the data processing implications of distributing face masks</p> <p>The CNIL has issued a statement on the data privacy concerns that may arise from the mass distribution of face masks in the community. The guidance acknowledges that the French municipalities will need to process personal data to inform the citizens of the mask distribution, arrange for the masks to be distributed and control these operations.</p> <p>The CNIL emphasises that municipalities should not hold files that list their citizens' contact details exhaustively and permanently, but can use specific pre-existing files for this purpose (such as housing tax files and the electoral list). The statement also provides practical guidance on the distribution of the masks, in particular if they are not to be posted anonymously, and the controls that may need to be put in place to ensure data security.</p>	The guidance is available here (only in French).	Data processing – public authorities
France	National Cybersecurity Agency of France (ANSSI)	27/4/20	<p>ANSSI announces project team developing StopCovid app pilot and clarifies its role in ensuring cybersecurity aspects of the app</p> <p>The French government launched a pilot project for the development of an app and related infrastructure</p>	The press release announcing the StopCovid project team is available here (only in French).	Mobile apps and new technology Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>(StopCovid). The project team includes, amongst others, the Public Health Authority of France, the National Institute for Research in Digital Science and Technology (INRIA), the National Institute of Health and Medical Research (INSERM), the ANSSI and a number of private organisations, such as Capgemini, Lunabee Studio, Orange S.A. and Withings. The project will be conducted in close collaboration with the CNIL.</p> <p>The StopCovid project aims at development of a contact tracing mobile app based on the following principles:</p> <ul style="list-style-type: none"> • the app will be one of the complementary elements in the overall strategy for managing the Covid-19 coronavirus health crisis and a support tool for public health authorities in phased lifting containing measures; • strict compliance with the data protection and privacy framework at EU and national level, as provided by French law and the GDPR, and in line with the European Commission's Toolbox on proximity tracking apps; 	<p>The press release describing the role of ANSSI is available here (only in French).</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • transparency, which includes publication of the developed app under open source license and ensuring transparency of algorithms, open source code, interoperability, auditability, security and reversibility of solutions; • digital autonomy of the public health system, including public control, protection and structuring of the health data to guide the response to the epidemic and accelerate medical research. • temporary nature of the project, with the lifespan corresponding, if deployed, to the duration of management of the Covid-19 epidemic. <p>At European level, the project will be carried out in close collaboration with national teams developing comparable applications in Germany, the fca, Italy, Spain and Norway, with expectation to develop interoperable solutions.</p> <p>The ANSSI also published its recommendations to INRIA on the information security aspects of the StopCovid pilot.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The recommendations include, amongst others:</p> <ul style="list-style-type: none"> • using secured electronic storage, hardware and software, to protect on the central server the pseudonymised data sent by the telephones; • designing and implementing secure architecture for all the components of the app and taking security measures against DDOS-type cyber attacks; • establishing access control mechanisms, ensuring accountability and traceability of actions carried out on the system; • carrying out security audits and checks by ANSSI during design and development of the app, along with a bug bounty program; • establishing a vulnerability management system for the app and the central server; • setting up cyberattack detection; • using the SKINNY-64/192 encryption algorithm for encryption of pseudonyms. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French supervisory authority (CNIL)	26/4/20	<p>CNIL issues opinion on StopCovid mobile app project</p> <p>The CNIL issued an opinion on the pilot project aimed at development of the contact tracing app under the supervision of the French government (StopCovid). The app will be voluntary and will be based on the proximity measurements of the Bluetooth technology, without processing geolocation data. The app will alert users of having been close to other app users who have been diagnosed with the Covid-19 coronavirus.</p> <p>The CNIL stated that under exceptional circumstances of the Covid-19 crisis management, it considers the system to comply with the GDPR if certain conditions are met. The CNIL calls for vigilance against the temptation of "technological solutionism" and stresses that the application can only be deployed if its usefulness is sufficiently proven and if it is integrated into a global health strategy.</p> <p>The CNIL also noted that the application should only be deployed and maintained temporarily if:</p> <ul style="list-style-type: none"> its usefulness has been confirmed and its use continues to be effective; 	<p>The press release is available here (in French only).</p> <p>The opinion is available here (in French only).</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • individuals must not experience negative consequences if they decide not to use the voluntary app, e.g. for access to tests and healthcare or such services as public transportation; • security of the mobile device and the app is guaranteed, and technical and organisational security measures are out in place; and • the retention period of data processed by the app must be limited. <p>The opinion notes that Art. 6(1)(e) GDPR (public interest) constitutes the most appropriate legal basis for processing under the application, in combination with Art. 9(2)(i) GDPR (public interest in the area of public health) and recommends to provide an explicit and precise legal basis for processing in national law at the time when decision is made to proceed with the pilot.</p> <p>The CNIL emphasises that specific details of the project are not known at this stage, and a new review by the CNIL will be required if the French parliament decides to deploy this solution.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French supervisory authority (CNIL)	22/4/20	<p>CNIL publishes opinion on health measures order</p> <p>The CNIL published an opinion on the draft order of the French Ministry for Solidarity and Health (<i>Ministre des Solidarités et de la Santé</i>) dated 21 April 2020 in relation to the organisational and operational measures in the health system necessary in response to the Covid-19 coronavirus pandemic.</p> <p>The draft order outlines proposals in relation to the management and centralisation of health data to prevent, diagnose, and treat the Covid-19 coronavirus, including on the Health Data Hub and the French national health data system (SNDS).</p> <p>The CNIL confirms that sufficient data privacy guarantees must be provided, and appropriate legal and technical measures must be implemented, in relation to the processing envisaged by the draft order. The opinion also notes that the use of data (and any processing under) the Health Data Hub requires an explicit legal basis.</p> <p>The CNIL confirmed it will also conduct a more detailed review of other aspects of the Health Data Hub that are not specific to the Covid-19 coronavirus pandemic.</p>	<p>The press release is available here (in French only).</p> <p>The opinion is available here (in French only).</p> <p>The order is available here (in French only).</p>	Data processing – public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French supervisory authority (CNIL)	17/4/20	<p>CNIL announces extended deadlines and prolonged authorisation procedures during the Covid-19 coronavirus crisis</p> <p>In this period of crisis, the CNIL will continue to give priority to cases related to the Covid-19 coronavirus epidemic. Most of the deadlines granted to its users to respond to its requests or decisions are extended to take into account this exceptional context. An ordinance also provides for the extension of the deadlines applicable to certain procedures implemented by the CNIL.</p> <p>Pursuant to Ordinance No. 2020-306 of 25 March 2020, as amended on 17 April 2020, the deadlines for examining requests for opinions and authorisation from the CNIL are suspended until 24 June 2020 for all applications submitted before 12 March 2020. The CNIL's silence on requests submitted during this period shall not constitute authorisation for data processing or favourable opinion on the draft texts.</p> <p>The CNIL will give priority, and respond within particularly tight deadlines, to any request for authorisation relating to research processing relating to on the epidemic, as well as any request for an opinion related to the Covid-19 coronavirus crisis.</p>	<p>The press release is available here (only in French).</p> <p>The Ordinance 2020-306 of 25 March 2020, as amended on 17 April 2020, is available here (only in French).</p>	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Other requests will be processed as usual, subject to the possible slowdown due to the containment measures. Organisations are invited, whenever possible, to provide requested additional documentation within the deadlines, preferably by electronic means.</p> <p>The same principles will apply to approvals and authorisations for codes of conduct, certification or binding corporate rules (BCR), requests for advice or for the instructions in relation to data breach notifications, namely: requests related to the Covid-19 coronavirus epidemic will be processed as a priority and other requests, as far as possible, within the usual time limits.</p> <p>The supervisory activities will take into account the constraints weighing on the organisations. Only serious situations requiring urgent investigations will trigger verification procedures. In addition, organisations may have the extended time limits to respond to follow-up requests for additional information.</p> <p>Unless otherwise provided by the CNIL, the deadlines to comply with a formal notice are suspended until 24</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>June 2020 for notices that did not expire before 12 March 2020.</p> <p>The CNIL can initiate any of these procedures in shorter time limits, for example, in the event of a serious infringement of the data subject rights or an urgent need to intervene to stop such infringement.</p>		
France	French supervisory authority (CNIL)	9/4/20	<p>CNIL publishes guidance on videoconference tools in the context of Covid-19 coronavirus</p> <p>The CNIL guidance recommends always reviewing the terms of use and avoiding videoconference tools that do not guarantee the confidentiality of communications or use personal data for other purposes. The CNIL warns about seemingly free tools that process personal data of users, including reusing data for advertisement or sharing with third parties. The guidance recommends that users:</p> <ul style="list-style-type: none"> • favour privacy-proof solutions (e.g. those certified by ANSSI); • read general terms and conditions applicable to the app, in particular in relation to personal data protection; 	The guidance is available here (only in French).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • verify that the app provider has implemented essential security measures (such as end-to-end encryption of communications); • limit the amount of information provided during registration; • check and customise the privacy settings of the app; • close the app when not in use, especially if the microphone or webcam are activated; and • mute your microphone and webcam when you are not using them and consider to cover or tape over the webcam, when not in use. 		
France	French supervisory authority (CNIL)	8/4/20	<p>CNIL addresses technologies based on the location data analysis during Covid-19 coronavirus crisis</p> <p>The CNIL's President Marie-Laure Denis has participated in a hearing on the Covid-19 coronavirus at the Law Commission of the National Assembly. The President addressed the issues related to Covid-19 research projects, the use of the location data, and contact-tracing apps.</p>	<p>The press release is available here (only in French).</p> <p>The introductory remarks are available here (only in French).</p>	<p>Mobile apps and new technology</p> <p>Data processing-location data</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Regarding technologies based on location data analytics, the CNIL's President reiterated the following main points:</p> <ul style="list-style-type: none"> • the EU and national legal data protection framework provides sufficient solutions for an adequate response to the crisis; • the use of solutions aimed at monitoring of individuals should be for a limited time, voluntary, and based on informed and genuinely free consent. Refusing the app should have no negative results for individuals; • introduction of a compulsory system for monitoring individuals would require a legislative provision and should, in any event, demonstrate its necessity to respond to the health crisis, proportionality and adherence to privacy protection principles, and be temporary; and • a chosen solution should represent only one of the elements of a wider healthcare response, be implemented with respect to privacy and personal data protection, create the conditions 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			for social acceptability of any potentially intrusive technique and guarantee the safety of people.		
France	French supervisory authority (CNIL)	1/4/20	<p>CNIL publishes recommendations regarding teleworking and security measures in the context of the Covid-19 coronavirus</p> <p>The CNIL recommends that organisations implement additional measures to secure information systems for teleworking. In particular, the CNIL recommends:</p> <ul style="list-style-type: none"> • updating security policies and documentation, include a set of minimum rules for teleworking, and communicating these new policies to employees; • if any changes are required to information system management in order to enable teleworking (for example, changing authorisation and authentication standards or remote administrator access), perform security risk assessment and address any identified risks; 	<p>The recommendations for organisations are available here.</p> <p>The recommendations for employees are available here. (only in French).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • equipping all workstations of employees, at a minimum, with a firewall, antivirus and tooling to block access to malicious websites; • setting up a VPN as soon as possible and enabling two-factor VPN authentication. <p>For organisations providing online services, the CNIL recommends:</p> <ul style="list-style-type: none"> • using the most recent versions of communication protocols to ensure confidentiality and authentication of the recipient server, for example HTTPS for websites and SFTP for file transfers; • applying the latest security patches to all equipment and software used (VPN, remote office solution, messaging, videoconferencing, etc.), monitoring the latest software vulnerabilities and the means to protect against them; • implementing two-factor authentication mechanisms for remotely accessible services; • regularly reviewing access logs for the remote services to identify suspicious behaviour; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> disabling direct access to any non-secure server interfaces and limiting the number of available services to a strictly necessary minimum in order to reduce the risk of cyberattacks. <p>The CNIL also published recommendations regarding teleworking on 1 April 2020 directed at employees, reflecting the recommendations outlined for organisations.</p>		
France	French supervisory authority (CNIL)	26/3/20	<p>CNIL will prioritise authorisation of research requests relating to Covid-19 coronavirus</p> <p>The CNIL announced that it will give priority to any authorisation requests for research projects related to Covid-19 coronavirus. The CNIL reiterated that any internal research projects related to Covid-19 coronavirus will not require any formalities; data controllers will need to only reflect data processing related to such new projects in their registers of processing activities. Other research projects should be verified against one of the reference methodologies of the CNIL (MR-001, MR-002 or MR-003); an organisation will need to issue a declaration</p>	The announcement is available here (only in French).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of conformity with one of these methodologies and can immediately proceed with the research.</p> <p>For situations when intended research project cannot comply with the requirements of these reference methodologies, organisations will need to apply to the CNIL for an authorisation. The CNIL provides additional guidance on how to apply and which documentation to provide, and commits to use the shortest review terms for a speedy handling of the application. The CNIL also provided a dedicated email address to facilitate requests and addressing any open issues related to such applications.</p>		
France	French supervisory authority (CNIL)	19/3/20	<p>CNIL clarifies legal framework applicable to sending government communications about Covid-19 coronavirus by telecom providers</p> <p>The CNIL provided a brief note clarifying the legality of personal data processing and sending text messages about Covid-19 coronavirus measures to the mobile phones of users in France. The CNIL notes that many individuals had received a text message on their phones reminding them of safety instructions related to combatting Covid-19 coronavirus, and that some had raised concerns with</p>	The CNIL's guidance is available here (only in French).	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the CNIL about privacy and data protection considerations of this communication.</p> <p>The CNIL clarified that sending text message about Covid-19 coronavirus measures was in compliance with a legal obligation on telecom operators to disseminate government messages to their subscribers to warn the public of imminent danger or major disaster. This did not entail sharing telephone numbers of subscribers with the Government and was in line with the requirements of the GDPR. The CNIL reiterated that the GDPR allows the processing of personal data without consent of individuals in certain cases, including when processing is done in the context of a legal obligation, for the purposes of public interest or for safeguarding of vital interests of individuals. Sending messages that are necessary for the purpose of Article L 33-1 of the Electronic Postal and Communications Code, in the context of the fight against the spread of Covid-19 coronavirus, is clearly part of this framework.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
France	French supervisory authority (CNIL)	6/3/20	<p>CNIL issues guidance for employers on processing personal data in relation to the Covid-19 coronavirus</p> <p>The CNIL provided guidance on conditions under which personal data and health data can be used in relation to the Covid-19 coronavirus. It outlined that data should only be collected to the extent required to manage exposure, and measures undermining individual privacy must be avoided. Systematic mandatory monitoring of medical sheets and body temperatures of employees, agents or visitors is not allowed; the same applies to the collection of medical surveys from employees.</p> <p>To implement measures that prevent occupational risks under the Labor Code, French employers can invite employees to communicate potential exposure or symptoms with health authorities. If an employee reports sickness or exposure to the Covid-19 coronavirus, the employer can record the employee's name, the date and measures taken, such as remote working or contact with the company doctor.</p>	The guidance is available here (in French only).	Data processing- employment Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Organisations may also be required to establish business continuity plans to maintain safety and the organisation's essential operations.</p> <p>Finally, the CNIL urges individuals and organisations to follow the recommendations of health authorities and to collect the health data of individuals only upon the specific request of the authorities.</p>		
France	Cybermalveillance	16/3/20	<p>Cybermalveillance publishes guidance on cybersecurity pitfalls and best practices in context of Covid-19 coronavirus</p> <p>The Cybermalveillance published guidance on best cybersecurity practices and pitfalls to avoid in the context of the Covid-19 coronavirus pandemic.</p> <p>Cybermalveillance.gouv.fr is a national platform governed by a public-private collaboration GIP ACYMA with the aim of raising cybersecurity awareness, and the prevention of and assistance to victims of cybercrime in public and private sectors other than critical infrastructure.</p> <p>The guidance reiterates the importance of being alert to phishing calls, text messages, emails and fake websites that can lead to installing malware on user devices and ransomware attacks, naming examples</p>	The guidance is available here (in French only).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of fake offers of protective clothing, remedies or travel certificates related to the Covid-19 coronavirus or fraudulent donation requests. Companies are warned against fraudulent bank transfer requests and risks of infecting corporate networks by ransomware.</p> <p>Organisations are called upon to implement additional security measures to prevent cyberattacks including:</p> <ul style="list-style-type: none"> • applying, without delay, security updates to devices connected to corporate networks; • enabling two-factor authentication procedures for teleworking; • enforcing strong password policies; • creating regular backups for data, including a backup not connected to the primary facility. 		
Finland	The Office of the Data Protection Ombudsman (the Finnish Ombudsman)	12/3/20	<p>Finnish Ombudsman clarifies data protection implications of processing personal data in relation to the Covid-19 coronavirus</p> <p>The Finnish Ombudsman issued a statement on privacy in relation to the Covid-19 coronavirus.</p> <p>The statement emphasises that data protection legislation does not restrict measures aimed at public</p>	The guidance is available here .	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>health protection or prevention of infectious diseases. However, data processing activities designed to limit the transmission of the Covid-19 coronavirus must take into account requirements of data protection law, in particular the principles of necessity and proportionality. The most important takeaways include:</p> <ul style="list-style-type: none"> • some data processed in relation to the Covid-19 coronavirus, such as information about the individual's health, diseases (including that an employee has contracted the Covid-19 coronavirus), disability or medical treatment, will be categorised as health data and therefore subject to the restrictions in relation to special categories of data under GDPR. Information that an employee has returned from a risk zone or is in quarantine is not health data, but still falls under the definition of personal data; • health data of employees may only be processed by specifically designated personnel who are subject to confidentiality obligations; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> employers may not name employees diagnosed with the Covid-19 coronavirus but may inform other employees about potential infection and instruct them to work from home; employers can inform third parties in general terms that an employee is prevented from carrying out their duties but may not disclose the name of employee who is diagnosed with the Covid-19 coronavirus or placed in quarantine. 		
Germany	German Parliament (Bundestag)	22/4/20	<p>Bundestag adopts resolution and report on tele- and video-conferencing for works councils</p> <p>The Bundestag approved a resolution and report from the Bundestag Committee on Labor and Social Affairs in relation to the draft law, "<i>Arbeit-von-morgen-Gesetz</i>" ("Work of Tomorrow Act" – <i>Gesetz zur Förderung der beruflichen Weiterbildung im Strukturwandel und zur Weiterentwicklung der Ausbildungsförderung</i>).</p> <p>The resolution and report proposed amendments to the draft law, including to:</p> <ul style="list-style-type: none"> allow certain works councils, employee representative bodies, and youth and trainee 	<p>The resolution and report are available here (in German only).</p> <p>The draft law is available here (in German only)</p>	<p>Cybersecurity and information security</p> <p>Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>representative bodies to attend meetings and adopt resolutions via video and telephone conferencing (applied retroactively from 1 March 2020);</p> <ul style="list-style-type: none"> • require participants to be able to confirm their presence at (video and telephone conferences) to the chairperson in writing; • prohibit recording of the video and telephone meetings; and • prohibit third parties from attending the meetings. 		
Germany	Federal Ministry of Health	27/3/20	<p>Federal Ministry of Health announced adoption of Covid-19 coronavirus-related legislative package</p> <p>The Federal Ministry of Health announced that the German Parliament adopted on 25 March 2020 the legislative package with broad range of measures to address the Covid-19 coronavirus pandemic. The package of legislative amendments includes measures that authorise the ministry to adopt ordinances decrees or ordinances to restrict cross-border travel, introduce reporting obligations for personal data (including health data) of travellers and</p>	The press release is available here (in German only).	Data protection-general guidance Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			other measures necessary for combatting the pandemic.		
Germany	Federal Commissioner for Data Protection and Freedom of Information (BFDI)	27/3/20	<p>BFDI publishes a compilation of guidance on data protection in relation to Covid-19 Coronavirus</p> <p>The BFDI, an authority responsible for supervision over compliance with data protection law by the public sector, and operators of telecom and postal services, published an overview of guidance notes issued by German supervisory authorities covering a large scale of data protection and cybersecurity issues that arise in relation to the Covid-19 coronavirus. The BFDI commits to continuously expanding and updating this overview.</p> <p>The BFDI stated that despite a clear priority that the society should be giving at this moment to combatting the Covid-19 coronavirus crisis, the protection of fundamental rights, including the rights to privacy and to personal data protection, are essential for free democratic society and should not be forgotten.</p> <p>The overview currently covers processing personal data in employment relationship, sharing mobile and geolocation data with government, processing data of</p>	The note is available here (in German only).	<p>Data protection-general guidance</p> <p>Cybersecurity and information security</p> <p>Data processing-employment</p> <p>Data processing-location data</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			visitors, general guidance on processing personal data and health data, and on working from home.		
Germany	German data protection conference (DSK)	3/4/20	<p>DSK publishes a resolution on data protection principles and the Covid-19 coronavirus management</p> <p>The DSK recognises that the Covid-19 coronavirus pandemic has been one of the greatest challenges faced by European societies in decades, and as the EU member states struggle to protect health of their people, it is essential for the stability of the state and society that citizens can rely on their fundamental rights and freedoms being only restricted to the extent and for as long as it is absolutely necessary and appropriate to effectively protect the health of the population. Intrusive measures must be reversible, limited in time and fall under the responsibility of legislature and not solely of the executive branch.</p> <p>The DSK reiterates the EU-wide uniform principles of data protection provided by the GDPR, in particular in Article 5, that can service as a guidelines for state actions and protect fundamental rights of individuals while not preventing an effective fight against the pandemic.</p>	The resolution is available here (in German only).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The DKS reiterated the following essential legal requirements for the processing of personal data in the times of the Covid-19 coronavirus pandemic:</p> <ul style="list-style-type: none"> • times of crisis do not change the fact that the processing of personal data must always be carried out on a legal basis, which means that the purposes of processing must be identified precisely; • any proposed measure must be assessed for its suitability, for example to detect infections, treat infected people or prevent new infections. An obligation on supporting organisations to report medically trained personnel to the healthcare authorities will be reasonable in the emergency situations. However, the suitability of measures aimed at understanding individual infection routes using telecommunications traffic data is doubtful; • any proposed measures must be necessary and priority should be given to less intrusive suitable measures, if available (for instance, data anonymisation). Preventive monitoring of the entire population would not likely to be 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>found a proportionate and legitimate data processing. Any measures that restrict freedom to a great extent must also be linked to special conditions (for example, a formal declaration of a health emergency);</p> <ul style="list-style-type: none"> • specific measures aimed at tackling the Covid-19 pandemic and entailing processing of sensitive data should be capable of being withdrawn after the end of the pandemic and should be generally limited in time. Personal data that are no longer required for the identified purposes must be deleted immediately; and • appropriate technical and organisational measures to protect the integrity and confidentiality of health data are necessary to prevent misuse of data and errors in processing. It is also important to inform the data subjects in a comprehensible way about the processing of their data. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Germany	German data protection conference (DSK)	13/3/20	<p>DSK publishes guidance for employers on data processing in relation to the Covid-19 coronavirus</p> <p>The DSK clarified that most personal data obtained in relation to the Covid-19 coronavirus is health data. The DSK stated that although processing of health data is subject to strict requirements, employers may process health data for the purpose of containing the pandemic provided that (i) the measures are proportional; (ii) there is a legal basis for the data processing; (iii) the purposes are clearly specified; and (iv) the data must be deleted when no longer necessary, the latest at the end of the pandemic.</p> <p>The DSK clarified that a possible legal basis for employers for processing health data of employees in relation to the Covid-19 coronavirus is Article 9(2)(b) GDPR and Section 26(3) sent. 1 of the German Federal Data Protection Act (BDSG) as the employer's duty of care under German employment law includes protecting the entire workforce against health threats and ensuring traceability of infections. The legal basis for processing health data of visitors or customers is Article 9(2)(i) GDPR and Section 22(1) no.1(c) BDSG.</p>	The press release is available here (in German only).	Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Examples of possible measures to contain and combat the Covid-19 coronavirus pandemic that may be considered legitimate under data protection law include scenarios for collecting information or employees or visitors:</p> <ul style="list-style-type: none"> • where infection has been detected or where there has been contact with a person who is known to be infected; • where a visit to a risk area (as classified by the Robert Koch Institute (RKI)) took place during the relevant period. 		
Germany	Federal Office of Information Security (BSI)	15/4/20	<p>BSI publishes security requirements for health apps</p> <p>The BSI announced development of technical guidelines (TR) addressing processing of sensitive personal data by mobile healthcare apps (BSI TR-03161). It is intended for broader application than the current Covid-19 coronavirus pandemic. It specifies that implementation of security requirements should be taken into account from the initial stages of developing software.</p> <p>The TR sets out minimum requirements for the safe operation of an application. The TR can be used to</p>	<p>The press release is available here (only in German).</p> <p>The TR is available here (only in German).</p>	<p>Mobile apps and new technology</p> <p>Cybersecurity and information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			meet the requirements of the approval process of the Federal Institute for Drugs and Medical Devices (BfArM) as part of a self-declaration by the developers.		
Germany	Federal Office of Information Security (BSI)	7/4/20	<p>BSI publishes an information package for individuals on secure networking in times of the Covid-19 coronavirus</p> <p>The BSI announced development of guidance addressing various aspects of the secure use of internet and digital networks during the Covid-19 pandemic.</p> <p>The BSI notes that due to the self-isolation and quarantine measures related to the pandemic, many people have become increasingly active in using digital tools and applications, such as video telephony, online games or streaming of films. The BSI information package aims at providing practical advice on good cybersecurity practices related to such use, for instance, securely setting up network devices, adhering to good password policies and securely creating user accounts. The BSI announced that it will be developing and expanding the guidance notes, which currently cover the following topics:</p>	<p>The press release is available here (only in German).</p> <p>The page with guidance on video conferencing, contactless payments, e-learning and safe streaming is available here (only in German).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • video calls; • contactless payments; • digital learning and tips for caretakers on safe use of smart devices by children; and • safe video streaming practices. <p>The press release also clarifies that the BSI is currently involved in development of a Covid-19 coronavirus app, including its penetration testing and supporting manufacturers in development of a related security model.</p>		
Germany	Federal Office of Information Security (BSI)	2/4/20	<p>BSI issues a brief statement on cybercrime and Covid-19 coronavirus and an update on protection against cyberattacks</p> <p>The BSI issued a brief statement discussing an increased number of cyberattacks in Germany that target the Covid-19 pandemic.</p> <p>Typical attacks include spam mails with malware claiming to provide information on Coronavirus and phishing emails requesting businesses or individuals to disclose confidential information or personal data via fake websites, claiming to come from healthcare or state aid institutions. The BSI further notes an</p>	<p>The statement is available here (only in German).</p> <p>The recommendations for protecting against cyberattacks is available here (only in German).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>exponential increase in registration of domain names containing pandemic-related keywords and recorded abuses of some of these domains by cyber criminals.</p> <p>The BSI warns users against downloading any Covid-19 apps or installing any software updates from unverified sources.</p> <p>The BSI further refers to its publication providing tips on recognising cyberattacks related to Covid-19 coronavirus and recommendations on protecting against cyberattacks.</p>		
Germany	Berlin DPA	2/4/20	<p>Berlin DPA created a dedicated information site on Covid-19 coronavirus guidance discussing home working</p> <p>The Berlin DPA has provided a section of its website with guidance related to data protection issues in the context of Covid-19 coronavirus.</p> <p>The website contains guidance on working from home during the pandemic and information about the restricted operation of the authority due to the pandemic measures.</p>	<p>The website is available here (only in German).</p> <p>The guidance on home working is available here (only in German).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Germany	Hamburg DPA	27/3/20	<p>Hamburg DPA publishes detailed guidance on data protection in the context of Covid-19 coronavirus</p> <p>The Hamburg DPA released detailed guidance, in form of the FAQs, addressing various aspects of privacy and personal data protection related to the Covid-19 coronavirus pandemic.</p>	The guidance is available here (in German).	Data protection-general guidance
Germany	Schleswig-Holstein DPA	24/3/20	<p>Schleswig-Holstein DPA publishes guidance on data protection issues of home working related to Covid-19 coronavirus</p> <p>The Schleswig-Holstein DPA released guidance to organisations on the privacy and data protection issues that arise in the context of increased working from home during the pandemic. The guidance points out that many employees will have to suddenly arrange a working place at home, and employers must ensure that appropriate attention is paid to protecting the personal data that employees are working with against unauthorised access at home or in transmission. Technical and organisational security measures are important for establishing routines when working on computer devices, with paper documents or when making calls. If a data breach occurs while working from home, employees must know how, and to whom, to report the breach.</p>	<p>The press release is available read here (only in German).</p> <p>The Guidance is available here (only in German).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Certain confidential work should not be carried out at home.</p> <p>Personal data should only be processed when necessary and companies should verify that there are no prohibitions under any agreement with counterparties that would prevent access to data from a remote working location.</p> <p>The Schleswig-Holstein DPA recommends that organisations should implement written policies for employees for remote working if they have not done so already.</p>		
Germany	Schleswig-Holstein DPA	18/3/20	<p>Schleswig-Holstein DPA discusses new Covid-19 coronavirus related registration obligations</p> <p>The Schleswig-Holstein DPA issued a note discussing data protection aspects of new registration obligations introduced recently to contain and combat the Covid-19 coronavirus pandemic.</p> <p>The Schleswig Holstein DPA reiterated that the GDPR does not prevent collection of personal data to combat the pandemic, but emphasised that necessary measures must be implemented to ensure proper handling of sensitive personal data.</p> <p>Competent authorities can take measures necessary to contain infections on the basis of their professional assessment and require personal data necessary for</p>	The guidance is available here (only in German).	<p>Data protection-general guidance</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			their specific purpose to be collected and processed. Competent authorities should provide entities with assistance on how to comply with these requests in manner compliant with data protection law.		
Germany	Rhineland-Palatinate DPA	31/3/20	<p>Rhineland-Palatinate DPA publishes a note on mobile tracking and other technical solutions for combatting the Covid-19 coronavirus pandemic</p> <p>The Rhineland-Palatinate DPA issued a brief note discussing various issues related to the use of technical solutions, including tracking of mobile location data, for combatting the pandemic.</p>	<p>The press release is available here (only in German).</p> <p>A note on mobile tracking in relation to Covid-19 is available here (in German).</p>	Mobile apps and new technology
Germany	Rhineland-Palatinate DPA	18/3/20	<p>Rhineland-Palatinate DPA announces limited availability due to the Covid-19 coronavirus pandemic</p> <p>The Rhineland-Palatinate DPA announced that due to general measures to combat the Covid-19 coronavirus pandemic, the DPA has reduced accessibility and anticipates delays in processing requests and other operations.</p> <p>When setting deadlines for businesses, imposing orders or calculating fines, the DPA will take into account the general restrictions on public life, the</p>	The announcement is available here (only in German).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			economic strain and prolonged administrative processes caused by the pandemic.		
Germany	Rhineland-Palatinate DPA	17/3/20	<p>Rhineland-Palatinate DPA discusses best practices for employers in relation to the Covid-19 coronavirus</p> <p>The Rhineland-Palatinate DPA published guidance on processing personal data in employment context in relation to the Covid-19 coronavirus, in particular health data as special category of data with higher standards applicable to processing.</p> <p>The DPA reiterates guidance by the DSK on this topic and refers to Section 20(3) of the Rhineland-Palatinate State Data Protection Act of 8 May 2018 as providing additional grounds for processing to comply with legal obligations under the laws relating to civil servants law, healthcare and occupational medicine.</p> <p>The guidance notes that:</p> <ul style="list-style-type: none"> a requirement to take and record body temperature of employees as a condition for their entering organisation's premises is not likely to be seen as measure necessary to comply with duty of care of the employer or employee, as increased temperature is not 	The guidance is available here (only in German).	Data processing- employment Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>solely connected with the Covid-19 coronavirus infection. The employer has many other options to fulfil its duty of care, for example by offering working from home options or access to a general physician or occupational doctor to check on flu-like symptoms for employees who previously visited high-risk areas;</p> <ul style="list-style-type: none"> • detailed surveys and questionnaires of all employees would not be proportionate, instead, employers can draw attention to the risks of staying in high-risk areas; • disclosing internally the names of employees infected by the Covid-19 coronavirus should be avoided. For contact investigation, employees can be asked to provide a list of contacts within organisation and the employer or public authorities can discretely approach persons on the list; • an assessment must be made of the data protection rights of data subjects before starting data processing. However, as the Covid-19 coronavirus has been classified as a 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			pandemic, public interest reasons are likely to outweigh interests of individuals on a case-by-case basis.		
Germany	Baden-Wuerttemberg DPA	27/3/20	<p>Baden-Wuerttemberg DPA published guidance on data protection-friendly communication tools in light of the Covid-19 coronavirus</p> <p>The Baden-Wuerttemberg DPA published guidance for organisations on data protection-friendly communication tools, with an emphasis on videoconferencing systems.</p> <p>When selecting a videoconference system, the Baden-Wuerttemberg DPA recommends that data controllers should ensure that the solution provider does not analyse the metadata related to video calls (e.g. who communicated with whom and when) or the content of the relevant communications, for its own purposes and nor should the solution provider share this data with third parties.</p> <p>The Baden-Wuerttemberg DPA also recommends using an "on-premises" videoconference system hosted on the organisation's own servers or in its data centre, as this would allow full control over all data flows and data collection. The Baden-Wuerttemberg DPA lists a number of open source, privacy-friendly tools available for this purpose.</p>	The guidelines are available here (in German).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Baden-Wuerttemberg DPA further recommends considering whether a videoconferencing solution will entail processing personal data outside the European Economic Area and ensure that appropriate safeguards are in place in case of cross-border data transfers.</p> <p>The guidance further reiterates that appropriate information should be provided to the users, deactivating recording of voice and video, unless there is a legal basis for such recording, in which case this should be made known to all participants at the beginning of the call. Participants should be offered an opportunity to participate in a call without an active video camera, especially if the call is made from their private premises.</p> <p>Alternatives to videoconferencing should also be considered, such as telephone or audio conferences, privacy-friendly and secure messengers, e-mail (if possible, secured by end-to-end encryption), text chats on privacy-friendly and end-to-end encrypted platforms or etherpads.</p>		
Germany	Baden-Wuerttemberg DPA	13/3/20	<p>Baden Wuerttemberg DPA publishes a FAQs on the Covid-19 coronavirus</p> <p>The Baden-Wuerttemberg DPA published frequently asked questions on processing personal data of employees and visitors in relation to the Covid-19</p>	The FAQs are available here (only in German).	<p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			coronavirus. The FAQs reiterate the guidance on the Covid-19 coronavirus adopted by the DSK. The FAQs further clarify the circumstances under which data have to be shared with healthcare authorities under the German Infection Protection Act (<i>Infektionsschutzgesetz</i>) and Article 6(1)(c) GDPR.		Data processing- public authorities
Greece	Hellenic Data Protection Authority (HDPa)	15/4/20	<p>HDPa publishes guidelines on remote working during Covid-19 pandemic</p> <p>The guidelines aim to help organisations ensure data security and compliance with the GDPR. In particular, they highlight employers' obligation to define procedures and train employees for remote working, accounting for nature and severity of risk, while outlining rules on internet access, email use, use of devices, and teleconferencing.</p> <p>They also point out the heightened privacy expectations of employees working from home.</p> <p>The Guidelines also recommend:</p> <ul style="list-style-type: none"> • taking measures regarding network access, e.g. using VPN and limiting access rights; • using encryption e.g. on usb sticks; 	<p>The press release is available here.</p> <p>The guidelines are available here. (both only in Greek)</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • firewalls and divisions between work-related data and personal data; • using strong WAP2 system when employees use WIFI; • avoiding storage of personal data using online services unless there are appropriate guarantees as to encryption, exclusivity of storage etc; • avoiding personal email accounts (if required applying effective encryption); • avoiding personal messaging services (if required choosing those with strong security features); • regularly updating security and software and using latest versions; • using secure and encrypted teleconferencing platforms, keeping links secure and taking care regarding treatment of personal data on a call; • backing up files; • locking devices. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Greece	Hellenic Data Protection Authority (HDPa)	14/4/20	<p>HDPa issues decision on modifying procedure rules</p> <p>The decision of 10 April 2020 (the Decision) modifies HDPa's own rules of procedure. It provides guidance on teleconferencing, while also highlighting that meetings conducted in relation to the procedure for imposing administrative sanctions, take place at HDPa's headquarters and are not made public. The Decision also notes that in cases where the HDPa exercises its powers under Article 58(2)(a) and (b) of the GDPR, it is entitled to issue decisions after a public consultation with interested individuals and third parties. It also states that, in exceptional circumstances, the HDPa may use teleconferencing for cases where a public consultation is required but the parties do not object to this.</p> <p>The Decision further notes that the HDPa may, either upon request or at its own option, carry out all or part of a procedure in private, where this is required, among other things, for reasons relating to benefits of minors, national security and safety, and for ensuring business secrecy</p>	The Decision is available here (only in Greek).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Greece	Cybercrime Division	3/4/20	<p>Cybercrime Division issues safe teleworking guide</p> <p>The safe teleworking guide provides key steps for employers and employees to ensure secure teleworking. More specifically, for employers, the guide recommends:</p> <ul style="list-style-type: none"> • the adoption of internal policies to manage security incidents; • the encryption of hard drives; • the training of employees in relation to teleworking. <p>In addition, the guide highlights:</p> <ul style="list-style-type: none"> • the need for specific plans for teleworking; • that employees should avoid using company devices for personal purposes. <p>The guide also recommends two-factor authentication.</p>	The guide is available here (only in Greek).	Cybersecurity and information security
Greece	Ministry of Digital Governance (MDG)	20/3/20	<p>MDG issues guidance on secure internet access</p> <p>The Greek Ministry of Digital Governance has issued guidance to help people stay safe online. The</p>	The guidance is available here (only in Greek).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>guidance highlights the increased risk of malware intrusion through alleged Covid-19 emails and links, and, amongst other things, urges users to pay close attention to any messages or links they receive which purport to relate to Covid-19.</p> <p>The guidance also asks citizens to trust official bodies to give them information about Covid-19 and highlights the falsehoods circulating on social media.</p>		
Greece	Hellenic Data Protection Authority (HDPa)	18/3/20	<p>HDPa issued detailed guidance on processing of personal data in the context of the Covid-19 coronavirus</p> <p>The HDPa states that the right to protection of personal data is not absolute and must be balanced against its functioning in society and against other fundamental rights, such as right to life and health. Public and private entities taking emergency measures necessary to prevent the dissemination of the Covid-19 coronavirus may process personal data in accordance with Art. 5, 6 and 9 GDPR, and none of their processing should be prohibited as a matter of principle, especially at this critical and unprecedented time.</p>	The guidance is available here (only in Greek).	Data protection-general guidance Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>In relation to processing of health data by private companies, the HDPa reiterates an obligation of employers to ensure the health and safety of their employees by taking necessary protective measures aimed at prevention of any serious, immediate and unavoidable risk. Employees must adhere to health and safety regulations. Under current circumstances, employers may process personal data of employees, suppliers or visitors, including asking to fill in questionnaires on their health status, recent travels to the affected areas or contacts with infected persons, while taking into account the principle of purpose limitation, proportionality and data minimisation.</p> <p>The HDPa clarifies that processing related to checking body temperature at the entrance to premises can only be applied in exceptional circumstances and cannot be systematic, permanent and of general nature.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
<p>Hungary [Updated as at 21 May 2020]</p>	Hungarian Government	4/5/20	<p>The Hungarian Government publishes a Governmental Decree specifying derogations from provisions regulating data subject requests and addressing data processing activities relating to the Covid-19 coronavirus</p> <p>The Hungarian Government Decree (No. 179/2020 (V.4)) provides that in relation to the processing of personal data for the purposes of the prevention, study, and detection of the Covid-19 coronavirus, data controllers can suspend the fulfilment of data subjects' requests under GDPR Articles 15 to 22 of the General Data Protection Regulation until the state of emergency is revoked in Hungary.</p> <p>The Decree contains further detail on information requirements and time limits for data subject access requests. For example, it enables data controllers to comply with GDPR Arts. 13 and 14 through publication of an electronic notice specifying the processing purpose, legal basis, and scope of data processing activities.</p> <p>The EDPB is investigating this approach, as has been specified in the EDPB recent plenaries.</p>	The Decree is available here (only in Hungarian).	<p>Data protection-regulator approach</p> <p>Data protection-general guidance</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Hungary	National Authority for Data Protection and Freedom of Information (NAIH)	10/3/20	<p>NAIH publishes a statement regarding the processing personal data in the context of the Covid-19 coronavirus</p> <p>The statement was issued in response to a number of queries as to the appropriate data processing practices when fighting the Covid-19 coronavirus.</p> <p>The statement focuses on the activities of both data controllers and processors and particularly addresses employers.</p> <p>It reminds data controllers, including the majority of employers, to comply with the GDPR and its principles, including when processing sensitive personal data such as employee health data. The statement covers accountability, necessity, proportionality, transparency and data minimisation requirements in general.</p> <p>More specifically, the statement notes business continuity plan requirements-expecting employers to develop and implement a plan covering employee communication, conduct and location of business changes and requirements to report contact with the Covid-19 coronavirus for the purposes of protecting the individual and colleague's health.</p>	The statement is available here .	Data protection-general guidance Data processing-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>If an employee reports possible exposure to the Covid-19 coronavirus the statement confirms that certain personal data may be recorded, for example name, date of report, location of travel, measures taken by employer. Whilst the NAIH confirms that questionnaires may be used if assessed by the employer in advance as being necessary and proportionate, data concerning medical history must not be requested nor may health documentation be collected.</p> <p>Potential legal bases and conditions for processing are listed as Art. 6(1)(f), 6(1)(e) and 9(2)(b) in the case of health data.</p> <p>The NAIH regards employer screening tests with any diagnostic device (including a thermometer) or the introduction of mandatory temperature measurement, generally involving all employees, as disproportionate – Covid-19 coronavirus status should be assessed by healthcare professionals and authorities.</p> <p>If based on the report of an employee or individual, considering all facts or on the basis of a risk assessment, if the employer finds it absolutely necessary (eg because some jobs are particularly affected by disease infection), the employer may call</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>for a test (and its results) by a health care professional. The statement flags potential legal bases and conditions in such case (GDPR Article 6(1)(f) or (e); GDPR Article 9(2)(h) and (3)).</p> <p>The NAIH confirmed that GDPR Chapter III rights continue to apply. See above for subsequent decree impacting Chapter III rights.</p>		
Iceland	Icelandic supervisory authority (Persónuvernd)	13/3/20	<p>Persónuvernd clarifies the uses of employee data in relation to Covid-19 coronavirus</p> <p>The Persónuvernd issued a statement in relation to data protection and the Covid-19 coronavirus. The statement confirms that any processing of health and personal data must be necessary and proportionate, and in accordance with data protection legislation.</p> <p>The Persónuvernd considers and comments on a number of processing situations, including:</p> <ul style="list-style-type: none"> • when an employee or student is quarantined; • when an employee or student is tested positive for the Covid-19 coronavirus; 	The statement is available here (only in Icelandic).	Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> the disclosure of information in relation to an employee's or student's absence due to quarantine or infection; completing questionnaires about foreign travel; the measurement of employees' body temperatures; general principles to follow when processing personal data in this context. <p>For example, the statement notes that names of quarantined individuals should not be disclosed unless strictly necessary, and employers should consider limiting the retention of any data collected in relation to the Covid-19 coronavirus.</p>		
Iceland	Icelandic supervisory authority (Persónuvernd)	6/3/20	<p>Persónuvernd clarifies the uses of employee data in relation to the Covid-19 coronavirus</p> <p>The Persónuvernd provided a statement on the use of employee data in connection with the Covid-19 coronavirus. The statement emphasises the importance of employees receiving sufficient information regarding the processing of their personal data. The statement encourages caution around</p>	The statement is available here (only in Icelandic).	Data processing-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			recording the minimum amount of personal data required for payroll and absence, and provided sample questions to ask employees.		
Ireland	Irish Data Protection Commission (Irish DPC)	3/4/20	<p>Irish DPC issues guidance on data protection in video-conferencing</p> <p>The Irish DPC issued brief guidance for individuals and organisations in relation to maintaining an adequate standard of data protection when video-conferencing. The guidance complements advice for individuals published on 12 March 2020 and 26 March 2020 on protecting personal data when working remotely and staying safe online during the Covid-19 coronavirus pandemic.</p> <p>The Irish DPC encourages individuals to adopt appropriate security practices, such as using up-to-date antivirus software and reviewing privacy policies prior to using a service to understand how personal data may be processed. The guidance also encourages individuals to consider the data protection and privacy rights of other individuals before posting or sharing a picture or video that contains the other party's image, voice or contact details.</p>	The guidance is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The guidance for organisations notes that employers should maintain clear and up-to-date organisational guidelines for video-conferencing and implement appropriate security controls.		
Ireland	Irish Data Protection Commission (Irish DPC)	26/3/20	<p>Irish DPC issues guidance on staying safe online during the Covid-19 coronavirus pandemic</p> <p>The Irish DPC published brief guidance for individuals in relation to protecting personal data online during the Covid-19 coronavirus pandemic.</p> <p>The guidance includes security hygiene tips, such as avoiding malicious URLs, and encourages individuals to share health data only with trusted recipients, such as government departments, healthcare professionals and public health officials.</p>	The guidance is available here .	Cybersecurity and information security
Ireland	Irish Data Protection Commission (Irish DPC)	25/3/20	<p>Irish DPC publishes a blog regarding data subject access requests and Covid-19 coronavirus</p> <p>The Irish DPC has posted a blog acknowledging the impact that Covid-19 coronavirus may have on the ability to respond to subject access requests, referencing the fact that some organisations will have re-deployed personnel and anticipating that delays may be unavoidable.</p>	The blog post is available here .	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>However, the DPC expects organisations to communicate with the data subject to explain the handling of their request (including regarding any delay/extension). The blog post reminds organisations of the potential under the GDPR to extend the timeline for response to a data subject request by up to 2 months.</p> <p>The DPC also suggests that the request for information is processed in stages, for example, providing electronic information initially with hard copy information following later for example.</p> <p>It is clear that the statutory requirements are not being waived so if problems meeting the deadline do arise, data controllers must ensure:</p> <ul style="list-style-type: none"> • that they do fulfil the response required as soon as possible; • reasons for not complying in full are documented; • reasons for not complying in full are clearly communicated to the data subjects; • the DPC is notified. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The DPC will take account of the facts of each case including any organisation specific extenuating circumstances will be fully taken into account.</p> <p>Finally, the blog post asks individuals making data subject requests to be aware of the potential delays that may be caused by the Covid-19 coronavirus.</p>		
Ireland	Irish Data Protection Commission (Irish DPC)	12/3/20	<p>Irish DPC issues guidance on protecting personal data when working remotely</p> <p>The Irish DPC published brief guidance for individuals on protecting personal data when working remotely due to the Covid-19 coronavirus. The guidance includes recommendations for individuals when working remotely and covers devices, such as USBs, phones, laptops, or tablets, the use of email, and tips for using cloud, network access and data sharing.</p>	The guidance is available here .	Cybersecurity and information security
Ireland	Irish Data Protection Commission (Irish DPC)	6/3/20	<p>Irish DPC publishes a blog post regarding compliance with data protection law in the context of the Covid-19 coronavirus</p> <p>The Irish DPC acknowledges that governments and organisations are taking steps to contain the spread</p>	The guidance is available here .	<p>Data protection-general guidance</p> <p>Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and mitigate the effects of Covid-19 coronavirus and that this may involve the processing of personal data.</p> <p>Whilst the Irish DPC notes that data protection law does prevent the provision of healthcare and the management of public health issues it highlights considerations which should be taken into account when handling personal data in the context of Covid-19 coronavirus including:</p> <ul style="list-style-type: none"> • measures taken involving the use of personal data, should be necessary and proportionate; • decisions should be informed by the guidance and/or directions of public health authorities, or other relevant authorities; • processing must be lawful (noting that a number of legal bases that may be relevant including Article 9(2)(i) GDPR and Section 53 of the Data Protection Act 2018 will permit the processing of personal data); <ul style="list-style-type: none"> ○ reliance on certain legal bases (e.g. Article 9(2)(i) GDPR) require implementation of safeguards which may include access limits, strict time limits for erasure, and other measures such as adequate staff 		Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>training to protect the data protection rights of individuals;</p> <ul style="list-style-type: none"> ○ employers legal obligation to protect their employees under the Safety, Health and Welfare at Work Act 2005 (as amended) can provide a legal basis for processing with Article 9(2)(b) GDPR where it is deemed necessary and proportionate to do so. The blog post clarifies that any data processed must be treated in a confidential manner i.e. any communications to staff about the possible presence of coronavirus in the workplace should not generally identify any individual employees; ○ a person's health data may be processed to protect their vital interest 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; ● organisations must be transparent including through provision of information to individuals describing, amongst other things, the purpose of processing and period of retention, in a 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>concise, easily accessible, easy to understand, and in clear and plain language;</p> <ul style="list-style-type: none"> processing in the context the Covid-19 coronavirus must ensure security of the data, in particular where health data is concerned. The Irish DPC notes that the identity of affected individuals should not be disclosed to any third parties or to their colleagues without a clear justification; only the minimum necessary amount of data should be processed to achieve the purpose; decision-making process should be documented. <p>The blog post includes a number of FAQs which act to clarify that:</p> <ul style="list-style-type: none"> employers have a legal obligation to protect the health of their employees and maintain a safe place of work. In the context of Covid-19 coronavirus, employers would be justified in asking employees and visitors to inform them if they have visited an affected area and/or are experiencing symptoms; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • more stringent actions, such as a questionnaire, require strong justification based on necessity and proportionality and on an assessment of risk. Consideration should be given to 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; • employers have a legal obligation to protect the health of their employees but employees also have a duty to take reasonable care to protect their health and the health of any other person in the workplace. Therefore, employers are justified in requiring employees to inform them if they have a medical diagnosis of Covid-19 coronavirus to allow necessary steps to be taken. However, recording of any health information must be justified, factual and limited to what is necessary to allow an employer to implement health and safety measures; • employers should follow the advice and directions of the public health authorities. This 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>may require the disclosure of personal data in the public interest to protect against serious threats to public health;</p> <ul style="list-style-type: none"> named disclosure to other employees of the fact that an employee has the Covid-19 coronavirus should be avoided to maintain confidentiality of the employee's personal data. Notification, on a no-names basis, that there had been a case of Covid-19 coronavirus could be justified; there are no data protection implications in drawing attention to Health and Safety Executive recommendations, if individuals have recently travelled to an affected area and/or are experiencing symptoms, and requesting that they take any appropriate actions. 		
Italy	Italian supervisory authority (Garante)	28/4/20	<p>Garante published a note on ransomware in relation to Covid-19 coronavirus</p> <p>The Garante notes that the extended use of online services and devices connected to internet by individuals due to the Covid-19 coronavirus health emergency goes along with "digital infection", fuelled</p>	The information note is available here (only in Italian).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>by attackers who spread malware for various illegal purposes. One of the most widespread and harmful types of malware is ransomware.</p> <p>The blog post clarifies the following:</p> <ul style="list-style-type: none"> • what is ransomware and its main types; • how it is typically spread (e.g. via attachments and hyperlinks in seemingly reliable emails, ad banners on websites, through software and apps, synchronisations between devices, data sharing in the cloud or using contacts directory to automatically send messages containing malware); • measures individuals can take to prevent ransomware infection (e.g. avoid opening emails from unknown senders, download apps from official sources, keep operating systems and frequently used software patched and updated, install antivirus and anti-malware applications on all devices and back up data regularly); and • recommendations for response to a ransomware attack (e.g. avoid paying ransom, seek help of forensic service, report the 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			ransomware attack to the police and notify Garante if personal data are affected by the attack.		
Italy	Italian supervisory authority (Garante)	19/4/20	<p>Garante publishes an overview of laws and regulations on the Covid-19 coronavirus that have impact on data protection</p> <p>The Garante published a detailed overview of the main provisions of the laws and regulations that have been adopted in response to the Covid-19 coronavirus pandemic and have impact on personal data protection rights of individuals and obligations of controllers in relation to processing personal data. The overview is being constantly updated by the Garante; the latest version is as recent as 19 April 2020.</p>	The overview is available here (only in Italian).	Data protection-general guidance
Italy	Italian supervisory authority (Garante)	31/3/20	<p>Garante draws attention to excessive disclosure of personal data of persons infected with the Covid-19 coronavirus on social media and in press</p> <p>The Garante addressed numerous complaints about dissemination on social media and in the press of personal data relating to people who tested positive</p>	The press release is available here (only in Italian).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>for the Covid-19 coronavirus, including their full names, home addresses and clinical details.</p> <p>The Garante warns against disregarding the legal norms and ethical rules aimed at protecting the privacy and dignity of people affected by disease. Garante calls upon information operators to comply with the requirement that published information must be "essential", to refrain from reporting the personal data of patients who do not play public roles, and publicise information on patients with public roles only to the extent knowledge of Covid-19 coronavirus testing, a positive result or sickness is important for to the public function of the individual.</p> <p>This does not involve effective information on the state of the epidemic or any communications that the health and civil protection authorities deem necessary to make on the basis of current emergency legislation.</p> <p>The Garante notes that an obligation to respect privacy and confidentiality of patients equally applies to users of social networks and administrators of local networks or social groups.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Italy	Italian supervisory authority (Garante)	29/3/20	<p>Garante discusses criteria for geolocation tracking of persons infected with Covid-19 coronavirus</p> <p>The Garante published a transcript of the speech given by the its president Antonello Soro on 29 March 2020 discussing the issues of tracking infected persons and a broader topic of processing personal data in relation to Covid-19 coronavirus pandemic. After addressing the impact of the pandemic on privacy and personal data protection, the Garante's president discussed which criteria could be used for deciding on the methods of locating infected or potentially infected individuals.</p> <p>Geolocation tracking of infected individuals Noting that there are many ways to implement geolocation tracking, the Garante recommends first looking into the least privacy-intrusive solutions that might be sufficient for the preventive purposes, such as using anonymised data.</p> <p>Where identification data are intended to be used, a regulatory provision, limited in time, proportionate to the purpose, based on a risk assessment and</p>	The transcript of the speech is available here (only in Italian).	Data processing- location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>providing adequate guarantees to individuals, must be put in place.</p> <p>The Garante suggests that the geolocation data on potential virus carriers (healthy or otherwise) should not be collected at all if there are no resources to analyse or make use this data.</p> <p>The Garante recommends to consider information assets available to the public authority and the complex supply chain in which contact tracing would be articulated. The data analysis (and possible re-identification) will require additional risk assessment and guarantees. Parties involved in the project should ensure that information and transparency requirements are complied with.</p> <p>The methods and scope of the proposed measures should be examined in view of their effectiveness, proportionality and adequacy, without blind trust into technological means.</p>		
Italy	Italian supervisory authority (Garante)	8/4/20	<p>Garante announces suspension of deadlines for proceedings</p> <p>The Garante extended the suspension of deadlines for concluding administrative proceedings, that were pending as at 23 February 2020 or which were</p>	The amended announcement is available here (only in Italian).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>initiated subsequently, until 15 May 2020 (though this date remains subject to change). The extension to 15 May 2020 follows an initial extension to 15 April 2020, as announced on 28 March 2020.</p> <p>The announcement notes that Garante maintains the right to take appropriate organisational measures to conclude proceedings and will give priority to cases considered urgent.</p>		
Italy	Italian government and trade unions	14/3/20	<p>Italian government and trade unions sign joint protocol on Covid-19 coronavirus measures in the workplace</p> <p>Several Italian trade unions together with the Italian President of the Council of Ministers and Ministries of Labour, Economic Development, and Health, signed a joint protocol in relation to the regulation of measures for the containment of the Covid-19 coronavirus in the workplace (the Joint Protocol).</p> <p>The Italian General Confederation of Labour (CGIL), Italian Confederation of Workers' Unions (CISL) and the Italian Labour Union (UIL) signed the Joint Protocol, which amongst other measures, considers the measurement of employees' body temperatures for permitting access to work premises and an</p>	<p>The CGIL's press release is available here.</p> <p>The CISL's press release here.</p> <p>The UIL's press release here.</p> <p>The Joint Protocol here (all only available in Italian).</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>obligation on the employee to inform the employer of any flu-like symptoms.</p> <p>The Joint Protocol confirms that real-time measurement of employees' body temperatures constitutes data processing and must be carried out pursuant to data protection legislation. For example, the Joint Protocol notes that identifying an employee who has exceeded the temperature threshold is permitted only if necessary to document the reasons for preventing the employee from accessing work premises.</p>		
Italy	Italian supervisory authority (Garante)	2/3/20	<p>Garante issues a statement on collection of personal data relating to Covid-19 coronavirus prevention</p> <p>The Garante issued a statement warning that private and public organisations should refrain from collecting information about Covid-19 coronavirus symptoms of their employees or company visitors, performing investigations on the health status of employees or their closest contacts, or demanding self-declarations from employees about being symptom-free.</p> <p>The Garante notes that emergency legislation adopted by Italian government in early February</p>	<p>The statement is available here (only in Italian).</p> <p>Emergency legislation adopted by Italian government in February available here (only in Italian).</p> <p>The short summary in English is available here.</p>	<p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>stipulates measures that can only be taken by institutions and persons that are qualified for execution of such function, including municipalities, designated health authorities and general health practitioners. These measures include fact gathering about Covid-19 coronavirus symptoms, required investigations of suspected cases and temporary isolation of individuals.</p> <p>The Garante reiterates that an obligation on employees to report to the employer any situation that might present danger to health and safety in the workplace remains unaffected. Recent operational indications by the Minister for Public Administration clarified that civil servants and employees of public agencies must report to the administration if they visited certain risk areas. The Garante notes that in this context, employers can invite employees to make such communications, where necessary, in order to direct these employees to come into contact with health services.</p> <p>Similarly, public service employees performing public-facing tasks (such as receptionists) who come into contact with a suspected case of the Covid-19 coronavirus, should communicate this to the</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			competent health services, also through the employer, and comply with the prevention indications provided by the health services.		
Latvia	Parliament of Latvia (Saeima)	16/4/20	<p>Saeima adopts new measures to address the spread of Covid-19 coronavirus</p> <p>Saeima has adopted new measures to address the spread of the Covid-19 coronavirus in Latvia, extending a state of emergency until 12 May 2020.</p> <p>The measures include the ability for the Centre for Disease Prevention and Control to transfer personal data to the Health Inspectorate, State Police and municipal police to enable them to control compliance with quarantine measures, and for State Border Guards to transfer completed certificates to State Police containing personal data of any person returning to Latvia, including the address of the place of self-isolation where that person can be reached.</p>	<p>The press release is available here.</p> <p>The measures are available here (only in Latvian).</p>	Data processing – public authorities
Latvia	The Data State Inspectorate (DVI)	20/3/20	<p>DVI issues brief guidance on processing of sensitive personal data in relation to Covid-19 coronavirus</p> <p>The DVI guidance clarifies that disclosure of health data is permitted if necessary for public health purposes. However, disclosure of information about</p>	The guidance is available here (only in Latvian).	Data processing- general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>individuals suffering Covid-19 Coronavirus and people at risk should be proportionate and reasonable.</p> <p>The DVI reiterates that GDPR will not apply to disclosure of information in a manner that does not allow the identification of the individual concerned, however, the DVI warns that identification of individuals on basis of disclosed information is often possible in cases of small communities that are characteristic for Latvia.</p> <p>The DVI further recommends obtaining actual information on the Covid-19 coronavirus outbreak only from trusted sources, such as official websites or social network accounts of public authorities.</p>		
Latvia	The Data State Inspectorate (DVI)	17/3/20	<p>DVI addresses processing of employee data in relation to Covid-19 coronavirus</p> <p>The DVI guidance discusses which GDPR ground for processing may be applicable in case of processing personal data of employees in this context. They consider processing necessary for purposes of public interest, protection of vital interests of individual in combination with processing necessary for public health protection of serious cross-border health threats.</p>	The guidance is available here (only in Latvian).	Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The DVI states that protection of personal data should not be an obstacle to the effective fight against the spread of communicable diseases, including the Covid-19 coronavirus.</p> <p>In this light, the employer is allowed to obtain information from employees as to whether they have been abroad for the past 14 days or whether they have been in contact with someone with the Covid-19 coronavirus, as this processing would be consistent with the legitimate health and public interest reasons and is necessary to protect other employees and clients.</p> <p>Employers have a duty under the Labour Law to prevent an employee who has the Covid-19 coronavirus from coming to the workplace and duties and to send the employee home and revert to the police if the employee does not follow the instructions of the employer. However, employers may not share information about the potential infection of a particular employee with other employees.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Luxembourg	Luxembourg Data Protection Authority (CNPD)	10/3/20	<p>CNPD clarifies processing of personal data of employees and visitors in relation to the Covid-19 coronavirus pandemic</p> <p>The CNPD published recommendations on processing personal data of employees and external persons, such as visitors, customers or suppliers, during the Covid-19 coronavirus pandemic. Information on a person's Covid-19 coronavirus health status qualifies as special categories of personal data subject to higher protection under the GDPR.</p> <p>The CNPD confirmed that employers have an obligation towards the health of their employees (article L312-1 of the Work Code) and are permitted to record the identity of individuals suspected of having being exposed to the Covid-19 coronavirus and detail the organisational measures taken in response.</p> <p>Employees should inform their employer if they think they may have been exposed to the Covid-19 coronavirus (Article L313-1 of the Work Code). However, the recommendations state that companies must refrain from collecting data in a systematic and</p>	The press release is available in French and in English .	Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>generalised manner, for example, through daily questionnaires on body temperature or symptoms.</p> <p>The CNPD provides, amongst other things, that employers may, as part of their health and safety obligations, collect and store the date and identity of the person suspected of having been exposed to the Covid-19 coronavirus and communicate the elements related to the nature of the exposure, which are necessary for any health or medical care of the exposed person, to the health authorities at the latter's request. Employers should, however, refrain from collecting information on possible symptoms experienced by an employee or visitor and their relatives in a systematic and generalised manner, or through individual inquiries and requests. Certain processing activities could, however, receive a lawful basis under future EU or Luxembourg law to address the outbreak of the Covid-19 coronavirus.</p>		
Netherlands [Updated as at 14 May 2020]	Dutch DPA	8/5/20	<p>Dutch DPA changes its position on processing employee health data in relation to the Covid-19 coronavirus</p> <p>The Dutch DPA expanded and amended its previous guidance on health checks of employees during the</p>	The guidance is available here (only in Dutch).	Data processing- employment Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Covid-19 coronavirus crisis and its Q&A on this topic (see below).</p> <p>The two most significant changes are:</p> <ul style="list-style-type: none"> • a clarification that some of the employment situations related to Covid-19 coronavirus pandemic will fall outside the scope of data protection law (and the Dutch DPA's supervision) and should be reviewed from an employment law perspective, for instance, if the employer intends to require employees to carry out temperature checks, leave the workspace if the employee develops Covid-19 Coronavirus-like symptoms during working hours or to undergo testing for Covid-19 coronavirus; • exclusively in relation to temperature checks, clarifying that merely taking an individual's temperature, without recording or further processing the results, would not represent processing of personal data and therefore not fall under the GDPR. However, some of these situations might still lead to privacy violations of employees. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The Dutch DPA reiterates the obligation on employers to provide a safe working environment and understands that employer may want to run health checks of employees during the pandemic in order to prevent spreading of infection in the workplace. However, employers are generally not allowed to process medical data of employees, may not ask employees about their health condition or perform health checks to verify it, and may not keep records of the reason of employee's sick leave.</p> <p>In this light, the Dutch DPA notes that organisations may not check their employees on Covid-19 coronavirus symptoms and only company doctors or occupational health practitioners may perform those checks.</p> <p>In the updated Q&A, the Dutch DPA retracted its previous guidance that, employers may send home employees showing signs of cold or flu due to the exceptional circumstances of the Covid-19 coronavirus pandemic. The current Q&A states that the Dutch DPA is not competent to provide guidance on this point as it reaches beyond processing personal data. The Dutch DPA notes that an answer will depend on the specific</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>employment relationship and refers generally to employment law for guidance.</p> <p>The Dutch DPA further established a section on its website dedicated to the Covid-19 coronavirus and all relevant guidance may now be found there. Amongst other things, the Q&A explicitly state that if an employee voluntarily informs an employer about being infected with the Covid-19 coronavirus, the employer is not allowed to record or share this information.</p>		
Netherlands	Dutch DPA	8/5/20	<p>Dutch DPA updates Q&A on the processing of personal data of employees in relation to the Covid-19 coronavirus and expands it with specific guidance on temperature checks</p> <p>The Dutch DPA updated its Q&A on processing of personal data of employees in relation to the Covid-19 coronavirus. The new Q&A supersedes the brief guidance published on 20 and 11 March 2020, in which the Dutch DPA had provided a strict interpretation of the applicable data protection law requirements.</p>	The Q&A is available here (only in Dutch).	<p>Data processing-employment</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The main points of the latest guidance are summarised below:</p> <ul style="list-style-type: none"> • checking whether employees have the Covid-19 coronavirus: <ul style="list-style-type: none"> ○ all employers (specifically including healthcare providers) must follow the guidelines established by the National Institute for Public Health and the Environment (RIVM), actively inform employees about these guidelines and provide the guidelines in all languages of the employees; ○ although in an answer directed at employees the Dutch DPA states, as previously, that employers may ask their employees to keep a close eye on their health, and contact the company doctor if necessary (this specific answer is available here), in guidance for employers the Dutch DPA states now more generally that it is not competent to provide an answer to this question and refers organisations to employment law requirements (this specific answer is available here). The Dutch DPA 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>further stated that, from a data protection law perspective, employees may follow instructions of the employer to perform self-checks of temperature as long as this would not amount to prohibited processing of special category of data. In practice this would mean that it should be up to the employees to take responsibility for and attribute consequences to the outcomes of the measurement, whether in line with the employer's instructions or not;</p> <ul style="list-style-type: none"> the Dutch DPA retracted its earlier position that employers may send employees home if they display symptoms of cold or flu, or if employer has doubts about their health condition and require employee to cooperate on this point. The latest position of the Dutch DPA is that it is not competent to provide guidance on this point and employers must seek answers in the employment law; the Dutch DPA modified its earlier guidance that employers may require an employee to contact a company doctor, occupational health service or general health practitioner to 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			perform a health check for Covid-19 coronavirus symptoms. The updated Q&A states that organisations should check their position in this respect from the employment law perspective. Sick employees can call in ill following usual procedures, for instance by taking contact with company doctor. If a doctor suspects the Covid-19 coronavirus infection, he or she will immediately contact the regional Public Health Service, which will, in consultation with employer, follow up with appropriate measures in the workspace.		
Netherlands	Dutch DPA	8/5/20	<p>Dutch DPA issues new guidance on taking temperature of employees and visitors and amends Q&A on processing employee data in relation to Covid-19 coronavirus</p> <p>The Dutch DPA updated its guidance on checking the temperature of employees during the Covid-19 coronavirus pandemic.</p> <p>The new guidance of the Dutch DPA states that the GDPR does not apply if the temperature is checked but the results are not processed in any manner, meaning they are not registered, shared with others (also within organisation) or saved in an automated</p>	The guidance is available here (only in Dutch).	Data protection-employment Data protection-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>system. The Dutch DPA notes that in practice the results of temperature checks are often shared internally or registered, for instance, in order to provide a person with access to the premises or refuse access. Therefore, automated systems that open entrance doors, allow access based on temperature checks or automatically process the results in other ways will fall under the scope of the GDPR.</p> <p>The Dutch DPA further states that the GDPR will most likely not apply to situations when employees, visitors or clients of the organisation are provided an opportunity to measure their own temperature. It reiterates that even if the temperature checks might not fall under the GDPR, they might still constitute a gross violation of a person’s fundamental right to privacy or other rights and freedoms, such as the right to physical integrity. It gives the example of violation of the right to privacy if, after the temperature is taken, an individual is not allowed to enter the premises and a queue of visitors can see that, and therefore form ideas about the health status of this individual.</p> <p>Consent</p> <p>The Dutch DPA restated its previous advice that temperature checks are in principle allowed on basis</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of explicit consent of individuals, noting that in many situations individuals are not free to give or refuse consents, such as in employment context.</p> <p>Employees</p> <p>In relation to employees, the Dutch DPA reiterated that also in the times of the Covid-19 crisis, employers are strictly prohibited from taking temperatures of employees. Having employee consents or permission of the Works Council to take temperature checks does not legitimise such processing. Health tests in the workplace can be performed, or health data of employees processed, exclusively by physicians or company doctors. The same rules apply to employees working for healthcare institutions.</p> <p>The Dutch DPA notes that employers should probably be able to require employees to monitor their own health, including temperature, and contact a company doctor if necessary, as well as require them to work from home, but explains that such situations fall outside the scope of the GDPR (unless they involve registration and processing of health data or consequences are attributed to taking temperature of</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>employees), so employers should evaluate their specific situation from an employment law perspective.</p> <p>Visitors and clients</p> <p>In relation to company visitors, the Dutch DPA generally confirmed its previous position that individuals working for other organisations (such as truck drivers delivering goods to the company) cannot provide a free consent to temperature checks.</p> <p>However, in addressing the same issue in relation to entrepreneurs (examples given point out that the DPA probably refers to SME), the guidance clarifies that checking temperature of visitors or clients before providing them access to premises (e.g. to company premises, shops or sport centers) is allowed if the entrepreneur can demonstrate that a free explicit consent has been obtained, which means that clients should be able to refuse consents without adverse consequences. The guidance states that this does not include situations when clients have no real choice or when no alternatives are provided (specifically pointing out that “free choice” excludes services provided by other parties).</p> <p>For the updated Q&A on this topic, please see above.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	28/4/20	<p>Dutch DPA publishes a note on anonymity of aggregated telecom data</p> <p>The Dutch DPA published a brief note regarding the new EDPB guidelines on the use of location data and tracing apps. The Dutch DPA reiterated that a contact tracing app may only be used when its purpose is clear, that the app would be the most effective means to achieve that purpose and where no less intrusive means to achieve that purpose are available.</p> <p>The Dutch DPA notes that the EDPB guidelines also make clear that achieving anonymisation is very difficult, in particular for location data. To explain this further, the Dutch DPA published an information note on anonymity of aggregated telecom data. The information note reiterates the requirement to anonymise data (i.e. to ensure that, despite any reasonable efforts of a third party that party is unlikely to succeed in singling out and re-identifying persons from the dataset). The note also provides an example of how individuals can be re-identified on the basis of analysis of aggregated telecom data.</p>	<p>The press release is available here (only in Dutch).</p> <p>The information note on anonymity of telecom data is available here (in English) and here (in Dutch).</p>	<p>Mobile apps and new technology</p> <p>Data processing-location data</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	24/4/20	<p>Dutch DPA clarifies that taking temperature of employees or visitors is generally not allowed and violators risk high fines</p> <p>Update 8 May 2020: the Dutch DPA created a dedicated page with general information and Q&A on temperature checks of employees and visitors that expands this guidance to include specific situations when taking temperature does not amount to processing personal data and would not fall under the GDPR (please see above).</p> <p>The Dutch DPA published on 24 April 2020 a brief note clarifying its position on practices in some organisations that require employees or visitors to measure their body temperature before entering the premises, for instance by using thermometers or thermal cameras.</p> <p>The Dutch DPA states that such practices are not allowed and constitute a serious offence under the GDPR.</p> <p>The regulator notes that taking temperature of individuals means processing their health data. Employers often believe that they can process health data if they have a consent of the individual, however,</p>	<p>The press release is available here (only in Dutch).</p> <p>Update: the link to the dedicated page on temperature checks for Covid-19 coronavirus is available here (only in Dutch).</p>	<p>Data protection-employment</p> <p>Data protection-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the Dutch DPA reiterates that obtaining valid consent in employment relationship is generally not possible due to an inherently unequal position of employees, who may feel pressured to give consent. The Dutch DPA reiterates that only medical doctors are allowed to run health checks, ask employees about their health or process their health data.</p> <p>In relation to company visitors, the Dutch DPA generally concluded the same, but only addressed a situation when a company intends to check body temperature of a truck driver who needs to enter premises to load and unload cargo. The Dutch DPA explained that the truck driver would also appear in an unequal position, being dependent on entering the premises to complete the delivery. Both the driver and their employer have an interest in gaining access to the premises, therefore the driver will feel compelled to give consent.</p> <p>The Dutch DPA advises employees of companies that measure their temperature to address this issue through the company's works council and the Data Protection Officer, if available. If the company doesn't stop such practices immediately, the Dutch DPA can</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			undertake an enforcement action and require the company to cease this data processing.		
Netherlands	Dutch DPA	22/4/20	<p>Dutch DPA concludes that none of the reviewed seven Covid-19 coronavirus contact tracing apps is sufficiently developed for proper assessment</p> <p>On 20 April, the Dutch DPA examined the design of seven mobile apps shortlisted by the Ministry of Health, Welfare and Sport (the Ministry) for tracing the source and contacts of individuals in relation to the Covid-19 coronavirus and concluded that no assessment can be made at this stage. The Dutch DPA clarified that the app requirements provided by the Ministry were unclear. The purpose of the intended app, its alignment with other governmental measures aimed to contain the pandemic, and the intended roles and responsibilities for data processing are not defined. In addition, the Dutch DPA noted that it cannot provide the proportionality assessment of the potential impact of deploying the app on the rights to privacy and personal data protection, in particular in relation to the less invasive alternatives.</p> <p>The Dutch DPA noted that all proposed apps were still at the early development stages, the app developers did not provide sufficient information about</p>	<p>The press release is available here (only in Dutch).</p> <p>The report is available here (only in Dutch).</p> <p>The press release about ongoing assessment is available here (only in Dutch).</p> <p>The letter of the Ministry is available here (only in Dutch).</p> <p>The annex to the letter describing selection process for the app is available here (only in Dutch).</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the app's design and could not demonstrate that their solutions provide appropriate technical and organisational safeguards for privacy and security for the app users and other individuals affected by the apps, for instance, how technological solution deals with false positives.</p> <p>The Dutch DPA announced earlier that it had been reviewing the apps for compliance with the requirements of the GDPR, in particular with the principles of proportionality, data minimisation, purpose limitation and data security. Once one app is selected by the government, the Dutch DPA will review its compliance with specifications and can prohibit its use in case of non-compliance with the requirements of privacy and data protection law.</p> <p>The Ministry published on 22 April 2020 a letter to the Parliament summarising the steps taken to identify possible technological solutions for addressing the Covid-19 coronavirus pandemic, including the mobile apps, and the follow up actions.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>These include:</p> <ul style="list-style-type: none"> • identifying clear and specific epidemiological requirements for digital support during various phases of the pandemic; • none of the apps and solutions involved in the previous selection procedure will be continued, however, the Ministry will establish a team of experienced app developers and experts on information security, privacy, human rights, national security and inclusion and task this team with development of an open-source based app for investigation of infection source and contact tracing; • the apps will be developed in close collaboration with the Dutch DPA, the Dutch NCSC, the College for Human Rights and the National Coordinator for Security and Counterterrorism and be subject to public consultation prior to deployment; • establishing a taskforce to analyse the behavioural aspects of the technological solutions; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> considering the introduction of statutory requirements that would prohibit third parties from making use of the apps mandatory. 		
Netherlands	Dutch DPA	15/4/20	<p>Dutch DPA publishes guidance on privacy aspects of video calling apps</p> <p>In view of increased use of videoconferencing due to remote working in the Covid-19 coronavirus pandemic, the Dutch DPA published a brief guidance note analysing privacy and data protection aspects of 13 commonly used video calling apps and a related table overview.</p> <p>The Dutch DPA has examined the most important data protection and privacy aspects of 13 commonly used video calling apps, including what data the app collects, how it processes this data, whether data are shared with third parties. The results of this high level examination is compiled in a high-level overview table mapping various privacy and data security aspects of the apps and the intended purposes of the apps use.</p> <p>The Dutch DPA recommends choosing a video calling app depending on the following criteria:</p> <ul style="list-style-type: none"> the purpose of the call; 	<p>The press release is available here (only in Dutch).</p> <p>The high level overview is available here (only in Dutch).</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> the number of intended call participants; sensitivity of the subject matter of the call in relation to the security of the app. <p>The Dutch DPA notes that for work-related video calls, the employer is responsible for providing a video app that protects privacy of both, employees and clients.</p> <p>The Dutch DPA recommends that organisations review the privacy and security aspects of video calling apps, consider using the paid version over the free apps if it offers better privacy and security options, and ensure they have a data processor agreement in place.</p> <p>The Dutch DPA also touches upon the issue of security and confidentiality of communications, options for end-to-end encryption and processing of conversation data and metadata. In addition, organisations should consider the location of organisations offering the app and of data processing, for instance, by exploring the options to process data on servers located within the EEA or hosting the app on organisation's own servers (self-hosting).</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	9/4/20	<p>Dutch DPA publishes a blog post on technological applications using anonymised data and location data in relation to the Covid-19 coronavirus</p> <p>The Dutch DPA emphasised potential benefits of deployment technological solutions to contain the spread of the Covid-19 coronavirus or forecast the needs of the healthcare sector in relation to the expected new infection cases. However, the DPA warned against indiscriminate deployment of technological solutions, in particular if they result in tracking device location data of individuals (noting that anonymisation of location data is almost impossible), which is prohibited without the individual's express consent.</p> <p>To facilitate organisations developing technological solutions in this area, the Dutch DPA has set up a special "corona team" that can provide quick support on possible ways to deploy such solutions with sufficient guarantees for privacy.</p>	The blog post is available here (only in Dutch).	Mobile app and new technology Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	2/4/20	<p>Dutch DPA clarifies that even at times of the Covid-19 coronavirus pandemic, patient's consent is required for access to medical records</p> <p>The Dutch DPA published a letter in response to the proposal of the Dutch Minister of Medical Care to adopt an administrative measure to circumvent strict statutory requirements to obtain patient's consent before sharing their electronic medical files stored in information systems of various healthcare providers. The measure would allow medical information exchange without patient's consent.</p> <p>The Dutch DPA considers this situation unacceptable and clarifies that in case no prior consent was given for sharing electronic health data, the Covid-19 coronavirus patient's consent must be sought at the time of admission in the hospital and verbal consent should be acceptable. If the patient is not capable to give a consent, the treating doctor may consult the medical file without the patient's consent.</p>	<p>The press release is available here (only in Dutch).</p> <p>The letter to the Minister of Health is available here (only in Dutch).</p>	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	1/4/20	<p>Dutch DPA states that the use of telecom data by the government during the Covid-19 coronavirus crisis should be embodied in a legislative act</p> <p>The Dutch DPA published a press release stating that the government is only allowed to use geolocation data of telecom users in the fight against the Covid-19 coronavirus when the use of data is laid down in an act of parliament.</p> <p>The Dutch DPA recognises that exceptional measures are being considered in exceptional times, such as the Covid-19 coronavirus pandemic, and that the limited use of location data under strict conditions may help the government to contain the spread of the Covid-19 coronavirus.</p> <p>However, the Dutch DPA stresses that the use of citizen location data by the government is very far-reaching, and it must be clear, in any case, that the measure for use of the data is proportionate with sufficient safeguards provided.</p> <p>The Dutch DPA considered the available options for sharing the telecom data with the government, such as asking user consent or anonymising the data, and</p>	The press release is available here (only in Dutch).	Data processing- location data Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>concluded that none of these options is available. Asking for consent is very cumbersome.</p> <p>Anonymising location data is impossible, as this process is never irreversible, according to the Dutch DPA. From an anonymised data set it is fairly easy to find out who the data belongs to if a person's home or work address are known.</p>		
Netherlands	Dutch DPA	20/3/20	<p>Dutch DPA announces a lenient approach to enforcing privacy and data protection obligations during the Covid-19 coronavirus pandemic</p> <p>The Dutch DPA issued an update on its approach to enforcing privacy and data protection obligations during the Covid-19 coronavirus pandemic. The Dutch DPA announced that it will give more space for public and private organisations to combat the pandemic and, where necessary, will expand the deadlines for responding to its requests, evaluating this on a case-to-case basis.</p> <p>The Dutch DPA names recent examples of its lenient approach towards healthcare organisations, such as allowing a healthcare provider to reach out, via an intermediary, to the former healthcare personnel in</p>	The statement is available here (only in Dutch).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>order to temporarily reinstate them as doctors or nurses in cases of critical personnel shortages.</p> <p>Another example is advising general health practitioners on the use of video chat apps for communicating with the Covid-19 patients, where the DPA explains how consumer apps like Skype or FaceTime can be used as an exceptional measure during the Covid-19 coronavirus outbreak (see for more details the guidance of the Dutch DPA of 18 March 2020, available here).</p> <p>The Dutch DPA stated generally that it will be understanding of the needs of organisations to focus their current resources on combatting the consequences of the Covid-19 coronavirus pandemic. Noting that fighting the virus and saving lives is a top priority, along with preventing the damage to the economy and society as a whole, the Dutch DPA stated that it will take a strict approach to enforcing privacy and data protection law. However, the supervisor emphasised that it will intervene in situations where the privacy of individuals is at real risk.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch DPA	18/3/20	<p>Dutch DPA issues guidance on secure remote working during Covid-19 coronavirus pandemic</p> <p>The Dutch DPA issued additional guidance on data security for remote working during the Covid-19 coronavirus crisis. The guidance provides four general tips for employees working from home, including:</p> <ul style="list-style-type: none"> • Secure home working environment: <ul style="list-style-type: none"> ○ use equipment, a laptop or tablet provided by the employer, if possible; ○ make additional working arrangements for this period with colleagues, clients and other contract parties; ○ use cloud services for document storage or email, in particular free services, with outmost care, as free cloud services might expose data to additional risks. • Measures to protect sensitive documents, such as customer lists or sensitive personal data on ethnicity, health or religion: 	The guidance is available here (only in Dutch).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none">○ take additional steps in relation to working with documents that contain sensitive information;○ make sure that any sensitive data that are only available on USB sticks or hard copies are scanned and placed on the organisation's server, and data on USB sticks are encrypted.● Using video and chat services:<ul style="list-style-type: none">○ use only the most secure means of communication (such as phone calls) for discussing sensitive information. If available, secure chat services that comply with strict security standards, such as apps used by healthcare organisations for conversations with patients, should be used;○ Fall back to consumer apps and chat services, such as FaceTime, Skype or Signal, should only be used in exceptional cases and subject to the necessity assessment and after taking necessary precautions, for instance, immediately		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>deleting chat history and ensuring that encryption settings are properly applied. Discussions via such media should mention as little sensitive data as possible, for example, calling parties should avoid using names of patients. The DPA also recommends informing individuals about privacy risks of using consumer apps and seeking their prior consent if calling with them via these apps.</p> <ul style="list-style-type: none"> • Phishing emails: <ul style="list-style-type: none"> ○ be vigilant about opening, clicking on hyperlinks or opening attachments in unexpected emails from unknown senders. The Dutch DPA warns about cyber criminals that are exploiting the Coronavirus crisis by sending phishing emails and recommends reporting suspicious emails to organisation's ICT departments. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Netherlands	Dutch National Cyber Security Centre (Dutch NCSC)	15/3/20	<p>Dutch NCSC issues guidance for organisations and their employees on cybersecurity aspects of remote working</p> <p>The Dutch NCSC issued guidance regarding cybersecurity aspects of working from home due to Covid-19 coronavirus measures.</p> <p>The recommendations for organisations include:</p> <ul style="list-style-type: none"> ensuring necessary network capacity and infrastructure, including both IT and telecom; assessing which employees should be available in the organisation to ensure IT support for teleworkers; updating incident response plans and processes to address risks due to potential shortage or limited availability of key personnel; making the use of secure connections to company networks mandatory (e.g. via VPN); verifying that telework solutions are tested and up-to-date; 	The guidance is available here (only in Dutch).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> implementing additional monitoring for applications that are critical for enabling remote work; utilising multi-factor authentication for access to company networks and strict password policy. <p>In addition, the Dutch NCSC recommends making employees aware of phishing related to the Covid-19 coronavirus and reminding them of company policies in relation to information security and the use of personal IT networks and equipment.</p>		
<p>Norway</p>	<p>Norwegian Datatilsynet</p>	<p>23/4/20</p>	<p>Norwegian Datatilsynet publishes response to consultation on NAV case management system</p> <p>The Datatilsynet published its response to the consultation on the Labour and Welfare Administration's (NAV) case management system (including testing of systems, automated decision making, collection of all income information some of which may typically obtained from the tax authority, streamlining of processes) during the Covid-19 pandemic (consultation letter dated 16 April).</p> <p>The response highlights that the proposed regulation has extensive implications for data protection and that</p>	<p>The response is available here (only in Norwegian)</p>	<p>Data processing – public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>it is crucial that measures are necessary and proportionate, even in exceptional circumstances.</p> <p>Amongst other things, the response considers that:</p> <ul style="list-style-type: none"> • NAV's collection and storage of all income information of the country's residents appears disproportionate in relation to the purpose for collecting that data and in any event, NAV must operate good control procedures such as access controls and logs and a continuous deletion process; • NAV should opt for anonymised or pseudonymised data instead of untreated personal data and should not use personal data just because it is easier to do so; • it should be explained in more detail how NAV shall ensure that the routines for testing / development meet the requirements for personal data security under these new conditions. • that decisions based on automated processing of data present an inherent risk of discrimination, algorithms should use correct data, it shouldn't contain hidden bias and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>individuals should have the right to request human assessment of their case;</p> <ul style="list-style-type: none"> regulations should clearly define application (i.e. to what sort of case) and be time limited (suggested six months). 		
Norway	Norwegian Datatilsynet	27/3/20	<p>Norwegian Datatilsynet issues statement on digital infection tracking system</p> <p>The Norwegian Datatilsynet issued a statement on the creation of an automated tracking system intended to trace cases of the Covid-19 coronavirus. The proposed system, approved by the Norwegian government, will rely on a mobile phone app built by the Norwegian Institute of Public Health to track the close social contact of individuals infected with the Covid-19 coronavirus.</p> <p>The Norwegian Datatilsynet acknowledges that the tracking system presents numerous privacy-related challenges and states that the mobile phone app must be voluntary to download. The statement also notes that public authorities should provide individuals with clear and comprehensive information as to the categories of personal data processed by the mobile phone app, the purposes of processing, the retention</p>	The statement is available here (only in Norwegian).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>periods, and the possibility and consequences of withdrawing consent for the mobile phone app.</p> <p>The Norwegian Datatilsynet emphasises that the legality of any public safety measure (such as the automated tracking system) is dependent on it constituting a necessary, appropriate and proportionate response in a democratic society. The statement confirms that the Norwegian Datatilsynet is monitoring developments in relation to the automated tracking system and will issue further statements following the public release of the mobile phone app.</p>		
Norway	Norwegian Datatilsynet	16/3/20	<p>Norwegian Datatilsynet issues FAQs on processing employee data in relation to the Covid-19 coronavirus pandemic</p> <p>The Norwegian Datatilsynet addressed numerous questions related to processing of personal data in employment context. The answers include:</p> <ul style="list-style-type: none"> data protection law permits processing special categories of data when necessary to carry out labour law obligations or rights. Information that someone is infected with Covid-19 coronavirus is health data. However, information that an employee has 	The guidance is available here (only in Norwegian).	Data processing- employment Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>returned from a "risk area" or has been quarantined (without giving further information about the cause) is not considered a health data;</p> <ul style="list-style-type: none"> employers may provide information within their organisation that employees have contracted the Covid-19 coronavirus or are in quarantine, but they should respect employees' confidentiality and use common sense when sharing this information. Such information should in principle not be shared externally. If a large number of employees are affected due to quarantine or other Covid-19 coronavirus related reasons, employers are recommended to draw a communication plan to inform customers and public of the situation; if one of the employees is infected or is in quarantine, the employer should follow advice given by the health authorities for follow-up and action in the business. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Norway	Norwegian Datatilsynet	11/3/20	<p>Norwegian Datatilsynet creates a dedicated section on their website with guidance related to the Covid-19 coronavirus pandemic</p> <p>The Norwegian Datatilsynet published a press release outlining the application of the GDPR to processing health data relating to individuals who have contracted the Covid-19 coronavirus. The authority has also established a dedicated section on its website providing answers to frequently asked questions and links to further guidance. The guidance highlights:</p> <ul style="list-style-type: none"> • in case of Covid-19 coronavirus infection, individuals must, in compliance with GDPR requirements, receive information about the processing of their personal data. Further clarifications are provided by the Norwegian Institute of Public Health; • requirements to perform a prior security assessment in relation to the security of technical environment and a DPIA for related data processing if a healthcare provider considers using video consultations with a Covid-19 coronavirus patient,. The current 	The guidance is available here (only in Norwegian).	Data processing- public authorities Data protection- regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>state of national emergency related to Covid-19 coronavirus pandemic will likely shift the balance towards justification of data processing or temporarily applying solutions with lower standards of security, however, when no immediate danger exists to life and health of individuals, data processing in this context should comply with GDPR requirements (such as entering into a data processing agreement with providers of video communication systems);</p> <ul style="list-style-type: none"> the Norwegian Datatilsynet may allow some leeway if an organisation cannot comply with a 72-hour deadline for a data breach notification. The data breach notification must indicate that delay is caused by the Covid-19 coronavirus crisis. 		
Poland	Polish supervisory authority (UODO)	21/4/20	<p>UODO publishes guidance for health institutions on exchange of information when conducting tests for Covid-19</p> <p>The UODO has published a brief note aimed to assist health institutions (i.e. laboratories, hospitals or sanitary and epidemiological stations) in determining</p>	The statement is available here (only in Polish).	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>which technical and organisational measures should be implemented in order to ensure appropriate level of security of their IT systems and sharing information in relation to individuals tested for Covid-19.</p> <p>The UODO reiterated that security measures must be based on a detailed analysis of the risks associated with the particular processing activity, and must take into account any national provisions on data security. To the extent not regulated by specific provisions, when choosing technical and organizational measures, the controller should take into account the state of technical knowledge, the cost of implementing the required safeguards, the nature, scope, context and purpose of processing, as well as the risk of violating the rights or freedoms of individuals.</p> <p>The UODO also emphasised that health institutions should limit access to personal data to what is necessary for them to carry out tasks and competencies specified by law.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Poland	Polish supervisory authority (UODO)	27/3/20	<p>UODO sends letter to Chief Sanitary Inspector in relation to data processing and the Covid-19 coronavirus</p> <p>The UODO's letter to the Chief Sanitary Inspector (CSI) responds to their letter of 20 March 2020 requesting clarification regarding legal basis for processing available to the CSI. The UODO highlights that the Act on Specific Solutions related to the Prevention, Restriction, and Control of COVID-19, and Other Contagious Diseases and Crisis Situations Caused by Them, all guidance, decisions, and recommendations of CSI are regarded as a sufficient legal basis for the processing personal data.</p> <p>The UODO flagged the need to comply with data protection laws, noted that DPOs should be used by the CSI and state inspection bodies to support processing of personal data and considered that special attention should be given to the purpose of data collection and disclosure of personal data.</p>	<p>The press release is available here.</p> <p>The letter is available here.</p> <p>(both in Polish)</p>	Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Poland	Polish supervisory authority (UODO)	17/3/20	<p>UODO issues a Covid-19 coronavirus guidance on working from home</p> <p>The UODO published a statement providing guidance on measures organisations should take whilst working from home.</p> <p>The statement suggests, amongst other things, that employees should:</p> <ul style="list-style-type: none"> • ensure they use secure passwords and antivirus products; • take particular care in using email; • use applications and software compliant with the company's security procedures; and • use established cloud service providers and networks. 	The statement is available here (only in Polish).	Cybersecurity and information security
Poland	Polish supervisory authority (UODO)	28/2/20	<p>UODO confirms that telecom operators may send messages about coronavirus</p> <p>The UODO issued a statement confirming that GDPR does not prevent companies from applying emergency measures prescribed by Polish government in relation to the coronavirus epidemic. UODO evaluated the proposed emergency measures</p>	<p>The statement is available here.</p> <p>The letter from UODO to the government is available here (both only in Polish).</p>	Data processing-public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and clarified that telecommunication companies should be allowed to send messages to mobile phones of users entering Poland in order to inform them about the spread of coronavirus and recommend actions to be taken in the event of suspected infection.</p> <p>The UODO emphasised that Article 21(a) of the Crisis Management Act 2007 contains an obligation on telecom network operators to send messages regarding the emergence of a crisis at the request of the director of the Government Centre for Security.</p>		
Poland	Polish supervisory authority (UODO)	12/3/20	<p>UODO clarifies application of Covid-19 coronavirus emergency law in employment context</p> <p>The UODO issued a statement on Covid-19 coronavirus and data protection. The statement notes that Article 17 of the "Act on Specific Solutions related to the Prevention, Restriction and Control of Covid-19, and other Contagious Diseases and Crisis Situations Caused by Them" (the Act) grants the Chief Sanitary Inspector authority to impose obligations on employers to take preventative or control measures</p>	<p>The Act is available here.</p> <p>The statement is available here (both only in Polish).</p>	Data protection-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and cooperate with other public administration bodies to combat the Covid-19 coronavirus.</p> <p>The Act also permits the Prime Minister to issue instructions to businesses in connection to the efforts to reduce transmission of the Covid-19 coronavirus.</p> <p>The UODO confirms that the Act is aligned with GDPR provisions in relation to public health and the prevention and spread of disease (Articles 9(2) and 6(1)(d)).</p>		
Romania	National Supervisory Authority for Personal Data Processing (ANSPDCP)	18/3/20	<p>ANSPDCP issues guidance on data protection in the context of Covid-19 coronavirus</p> <p>The ANSPDCP issued guidance on data protection in the context of the Covid-19 coronavirus. The guidance reminds controllers of the need to ensure that processing of health data meets with a condition set out in Article 9 GDPR, including, processing necessary for the purpose of fulfilling the obligations and exercising specific rights of the controller or data subject in the context of employment (subject to certain further conditions).</p> <p>Amongst other things the guidance reminds controllers of their obligation to:</p>	The guidance is available here (only in Romanian).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> inform data subjects of the processing activities in accordance with Articles 13 and 14 of the GDPR, in each case, in a concise, transparent, intelligible and easily accessible form, using clear language; put in place technical and organisational measures to ensure adequate security. <p>The guidance also highlights Article 23 GDPR (Restrictions) and the potential to restrict certain data subject rights on the basis of EU or Member State law for, amongst other things, safeguarding public health.</p>		
Russian Federation	Ministry of Digital Development, Communications and Mass Media (Mincomsvyaz)	22/4/20	<p>The Mincomsvyaz announces a roll-out of a federal platform for issuing digital passes during the Covid-19 coronavirus lockdown</p> <p>The Mincomsvyaz has launched a federal platform for issuing digital passes for individuals during the Covid-19 Coronavirus pandemic. The temporary or permanent digital passes, in the form of QR codes, can be provided to employees of critical infrastructure organisations (via the organisation's account) or the users of the e-Gov mobile app STOPCoronavirus and are valid only in combination with individual's identification documents. The platform had been</p>	The press release is available here (only in Russian).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			successfully tested in the Moscow region and will now be expanded to cover an additional 21 regions of Russian Federation.		
Russian Federation	The Government	23/3/20	<p>The Government announced plans to track geolocation data of individuals to tackle spread of Covid-19 coronavirus</p> <p>The Government instructed the Ministry of Digital Development, Communications, and Mass Media to establish a system that will track individuals who were in contact with individuals infected with Covid-19 coronavirus based on geolocation data of mobile devices provided to the government by telecom operators. The intended system will include notification to individuals about the fact that they had been in contact with an infected person and should take measures aimed at self-isolation. This information will be also shared with operational emergency units.</p> <p>The new system should be operational by 27 March 2020.</p>	The statement is available here (only in Russian).	Data processing-location data Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Russian Federation	Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor)	17/3/20	<p>Roskomnadzor issues a brief warning about phishing attacks abusing the topic of Covid-19 coronavirus</p> <p>The Roskomnadzor issued a brief statement warning about high risks related to the intensified activity of cybercriminals who use the topic of the Covid-19 coronavirus pandemic to defraud companies and individuals. Attackers and fraudsters have been sending messages with false recommendations for the prevention of the disease, disseminating fake information or installing malware on devices of addressees on a massive scale. The Roskomnadzor reiterates basic security hygiene rules to protect against such attacks, such as not opening attachments or clicking the links in suspicious emails, trusting only reliable sources of information, such as websites of public authorities and verifying the authenticity of a web shop before placing an online order.</p>	The statement is available here (only in Russian).	Cybersecurity and information security
Russian Federation	Federal Service for Supervision of Communications, Information Technology and	10/3/20	<p>Roskomnadzor clarifies the use of thermal imagers for Covid-19 coronavirus checks of employees and visitors</p> <p>The Roskomnadzor has issue a statement about the use of thermal image cameras by private</p>	The statement is available here (only in Russian).	Data protection-employment Data protection-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
	Mass Media (Roskomnadzor)		<p>organisations to measure the body temperature of employees and visitors.</p> <p>The Roskomnadzor clarify that body temperature is special category of personal data under Russian data protection law, as it can reveal information about the state of individual's health. Processing of health data in employment relationship without data subject's consent is allowed in accordance with the statutory provisions of labour law. Art. 88 of the Labour Code of the Russian Federation provides the employer is not entitled to request information about employee's health status unless it concerns the data indicating whether employee is capable to perform work. The Roskomnadzor concludes that Covid19-coronavirus falls under this exemption and an employee's consent to measuring body temperature is not required.</p> <p>Visitors who do not have an employment relationship with the organisation can give their consent to the processing of information about their body temperature through specific actions, for instance in their evident intention to visit the organisation. If an elevated body temperature is detected, the visitor should be referred for a consultation with a doctor.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Employees and visitors must be informed about the body temperature checks, for instance by an announcement displayed at the entrance to the organisation.</p> <p>The Roskomnadzor recommends deleting the images not later than a day after their collection, as the purpose for processing has been achieved.</p> <p>The Roskomnadzor further clarifies that regional decrees and regulations that are adopted for the purpose of combatting the Covid-19 coronavirus pandemic might include additional grounds for processing health data in this context.</p>		
Spain [Updated as at 21 May 2020]	Spanish supervisory authority (AEPD)	7/5/20	<p>AEPD publishes report on privacy risks in technologies responding to Covid-19 coronavirus</p> <p>The AEPD published a preliminary report on the use of technologies developed in response to the Covid-19 coronavirus pandemic.</p> <p>The AEPD confirmed that any processing of personal data by such technologies must have a clearly defined purpose, and to the extent a technology is developed in response to the Covid-19 coronavirus, the technology must be based on a coherent strategy based on scientific evidence and carried out in</p>	<p>The press release is available here.</p> <p>The study is available here. (Both only in Spanish)</p>	<p>Mobile apps and new technology</p> <p>Data processing-location data</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>accordance with GDPR and the regulatory frameworks established by health authorities.</p> <p>The AEPD considered seven systems or approaches:</p> <ul style="list-style-type: none"> • geolocation data collected by telecommunications operators; • mobile geolocation data collected from social networks; • apps, websites and chat-bots designed as an interface for self-diagnosis or making appointments; • voluntary infection reporting and information apps; • Bluetooth contact tracing apps; • digital immunity passports; and • infrared cameras. <p>The report noted that contact tracing applications present particular privacy risks, including in the possible mapping of personal relationships, re-identification of location of individuals, collection of third party data, and in the fragility of protocols involved in information exchange. Amongst other</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>things, the AEPD highlights that centralised technological solutions appear to provide less privacy than distributed or decentralised solutions.</p> <p>The AEPD also notes that, though potentially useful in occupational risk prevention, the use of infrared cameras may give rise to possible discrimination, public dissemination of health data, and create a false sense of reduced risk. The report confirms that use of infrared devices must be carried out in accordance with criteria published by health authorities.</p>		
Spain	Spanish supervisory authority (AEPD)	30/4/20	<p>AEPD publishes statement on temperature checks</p> <p>The AEPD published a statement on the use of temperature checks at workplaces, shops and other establishments, which confirms that processing an individual's temperature constitutes processing of sensitive personal data and must be carried out in accordance with GDPR and criteria published by health authorities.</p> <p>The AEPD expresses concern that the use of temperature screening could lead to unjustified workplace discrimination, especially if an employee is barred from entering their workplace. The statement notes that consent should not be relied upon as the</p>	The statement is available here (only in Spanish).	Data processing-health status Data processing-employment

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>legal basis for such processing if affected individuals cannot refuse to provide consent if to do so would prevent access to places of work, education and commerce or using public transport (ie consent is not freely given). Rather, obligations of employers to guarantee safety of works would be a more appropriate legal basis. The guidance confirms that legitimate interest is not an acceptable legal basis to justify temperature testing.</p> <p>The statement also highlights the importance of purpose limitation, data accuracy, and ensuring individuals are able to exercise their data subject rights.</p>		
Spain	Spanish supervisory authority (AEPD)	14/4/20	<p>AEPD issues blog post on the processing of personal data in emergency situations</p> <p>The AEPD published a blog post that sets out guidance for the processing of personal data in emergency situations, although this is not limited to (and does not specifically mention) the Covid-19 coronavirus pandemic.</p> <p>The blog post clarifies that not all data that can be collected during an emergency will be useful in dealing with that emergency. Organisations must use</p>	The blog post is available here (in Spanish) and here (in English).	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>objective parameters to select the personal data that is appropriate to address the issue at hand, ensuring that this is of sufficient quality and accuracy. The AEPD emphasises that this only personal data should be processed and no more.</p> <p>The blog post further sets out the importance of effective decision making and evaluating whether the benefits of the personal data processing will lead to real improvements, before any action is taken. The AEPD highlights a particular risk that any excessive personal data collected could fall into the wrong hands and be used against the collecting organisation.</p>		
Spain	Spanish supervisory authority (AEPD)	7/4/20	<p>AEPD issues recommendations on the data protection impact of working remotely</p> <p>The AEPD has issued recommendations on data protection and security in the context of teleworking. The recommendations confirm that an organisation, as controller, may determine that its employees can carry out their duties remotely, but that any employer doing so must consider many factors including the rights and freedoms of individuals whose personal data it processes.</p>	The recommendations are available here (only in Spanish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The recommendations set out specific behaviours that those in charge of such an organisation should adopt. These include, amongst others, implementing an information protection policy that covers teleworking and remote access, providing training to employees, entering into a remote working agreement with those employees, performing due diligence on service providers, restricting access to information to that necessary for the individual to perform their role, periodically re-configuring devices, managing data protection and security, monitoring access to the corporate network, maintaining the security of equipment and devices used and consider using lawful employee monitoring techniques where necessary.</p> <p>The AEPD also provides recommendations of content to include in policies for employees when working remotely too. These include respecting any information protection policy implemented by their employer, maintaining the security of devices through password protection and refraining from connecting to unsecured Wi-Fi networks, minimising paper-based working, shielding computer screens and saving documents on their organisation's cloud storage</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			system (rather than locally). Employees are also encouraged to contact their organisation's data protection officer with queries or for further guidance.		
Spain	Spanish supervisory authority (AEPD)	2/4/20	<p>AEPD publishes blog post on data breach notifications during Covid-19 coronavirus emergency</p> <p>The AEPD published a note where it clarifies that, despite the fact that Royal Decree No. 463/2020 of March 14 2020 Declaring the State of Emergency for the Management of the Health Crisis Situation caused by Coronavirus suspended the terms of administrative procedures of public sector entities, the obligation to notify a personal data breach to the AEPD and, where applicable, to data subjects affected by the breach, as provided under the GDPR and within the terms established by the GDPR, remains in force.</p> <p>The AEPD reiterates that emergency situation due to the Covid-19 coronavirus pandemic cannot mean a suspension of the fundamental right to the protection of personal data.</p>	The blog post is available here (in Spanish) and here (in English).	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Spain	Spanish supervisory authority (AEPD)	26/3/20	<p>AEPD issues statement on the collection of health and geolocation information in relation to Covid-19</p> <p>The AEPD issued a statement on the collection of health and geolocation data in relation to the Covid-19 pandemic. The AEPD highlight that the pandemic is leading to a high volume of processing of health data and, whilst data protection legislation should not impede the fight against the pandemic by competent authorities, the emergency situation cannot result in a suspension of the fundamental right to the protection of personal data.</p> <p>The AEPD statement reiterates the criteria that must be applied in order to process personal data lawfully. In particular the AEPD considers the legal basis required to process health data in connection with Covid-19, such as where the processing is carried out in the public interest or to protect the vital interests of affected persons or third parties. Private organisations are reminded that, where they are collaborating with public authorities, they should only process personal data in accordance with the instructions they receive.</p> <p>The AEPD also contemplates the sharing of geolocation data with public authorities to enable the</p>	The statement is available here (in Spanish) and here (in English).	Data processing- location data Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>pandemic to be monitored and advises telecoms providers that they should only provide geolocation information to public authorities and no other data they hold on citizens.</p>		
Spain	Spanish supervisory authority (AEPD)	16/3/20	<p>AEPD warns websites and apps offering Covid-19 coronavirus advice and self-assessment in violation of data protection law</p> <p>The AEPD issued a statement on websites and mobile apps that are offering Covid-19 coronavirus advice and self-assessment. The AEPD has identified certain websites and apps that do not provide the necessary information to data subjects about collecting their personal data, such as the name of the data controller and the purpose of processing.</p> <p>The statement warns that the AEPD will start investigations to verify the lawfulness of the processing, identify responsible subjects and will consider imposing sanctions.</p>	The statement is available here (only in Spanish).	<p>Mobile apps and new technology</p> <p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Spain	Spanish supervisory authority (AEPD)	12/3/20	<p>AEPD publishes FAQs for employers on data processing related to Covid-19 coronavirus</p> <p>The AEPD issued a document containing responses to a number of frequently asked questions (FAQs) it has received relating to the Covid-19 coronavirus.</p> <p>The FAQs highlight that the GDPR allows for the processing of health data without consent in situations of public interest and affecting public health under certain conditions and that data protection law should not be used to hinder or limit the effectiveness of measures taken by the health authorities.</p> <p>The FAQs also confirm that an employer has a mandatory obligation to verify the health status of employees and this verification should be performed by healthcare professionals or medical staff.</p>	The FAQs is available here (only in Spanish).	Data processing- employment Data processing- health status
Spain	Spanish supervisory authority (AEPD)	12/3/20	<p>AEPD addresses cybersecurity risks related to Covid-19 coronavirus pandemic</p> <p>The AEPD published a blog post on the likelihood of cyber criminals taking advantage of the current emergency situation by launching phishing attacks through email, instant messaging services or other means.</p>	The blog post is available here (only in Spanish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The AEPD recommends that individuals verify the email address and content of the messages they receive as well as being cautious of requests for personal data within websites reached through links provided in those messages. The AEPD also commented that cyber criminals will likely impersonate governments or other official bodies such as the Ministry of Health, pretending to provide help and advice.</p>		
Spain	Government of Spain	3/5/20	<p>Spanish Government announces transition plan for lifting measures established in response to the Covid-19 coronavirus pandemic</p> <p>The Spanish Government published a transition plan, which was approved on 28 April 2020, and establishes the main parameters, key measures, and necessary instruments for easing and amending the measures established in response to the Covid-19 coronavirus pandemic.</p> <p>The transition plan confirms that any containment mechanisms and in particular contact tracing and quarantining must guarantee the anonymity and privacy of information.</p>	<p>The press release is available here.</p> <p>The transition plan is available here.</p> <p>Associated FAQs are available here.</p> <p>(All only in Spanish)</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Spain	Ministry of Health, Consumption and Social Welfare (the Ministry of Health)	12/5/20	<p>Spanish Ministry of Health adopts measures on epidemiological surveillance during transition period</p> <p>The Ministry of Health adopted an order that outlines measures in relation to epidemiological surveillance of the Covid-19 coronavirus during the transition phase (see transition plan above).</p> <p>The order applies to the identification, diagnosis, monitoring, and management of cases of Covid-19 coronavirus, and outlines certain disclosure obligations to competent public health authorities in relation to suspected or positive diagnoses.</p> <p>Article 9 of the order states that personal data processed in the application of the order will be done in accordance with GDPR, including compliance with Art. 14 GDPR (information requirements). The order acknowledges that epidemiological monitoring and surveillance amounts to essential public interest in public health and the protection of vital interests for the purposes of legal bases and conditions of processing under the GDPR. Article 9 of the order also notes that the Ministry of Health will guarantee mandatory security measures resulting from a corresponding risk analysis and accounting for the</p>	The order is available here (only in Spanish).	Data processing- health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			special category nature of the personal data in question.		
Spain	Ministry of Economic Affairs and Digital Transformation (the Ministry)	6/4/20	<p>Spanish Ministry of Economic Affairs and Digital Transformation launches self-assessment app for Covid-19 coronavirus symptoms</p> <p>The Ministry has published a press release confirming that a self-diagnosis app, named "AsistenciaCOVID-19", is now available in five further autonomous communities in Spain alongside the city of Madrid, where the pilot scheme was carried out.</p> <p>The app is available on mobile or desktop. It allows users to self-diagnose any symptoms, review recommendations and receive reminders to monitor their health status. The aims of the app are to offer health information to citizens while keeping emergency care phone lines as free as possible. It is not intended to replace medical diagnosis or emergency care.</p> <p>The data collected by the app includes the user's geolocation information, to suggest local resources where necessary, but the Ministry confirms that the intention of the app is not to monitor compliance with social distancing. The data collected by the app will</p>	The press release is available here (only in Spanish).	Mobile app and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			be available only to healthcare professionals and authorised competent authorities and it will be kept only for the duration of the crisis (then anonymised and used for research purposes for up to a further two years).		
Spain	Spanish National Cybersecurity Institute (INCIBE)	5/5/20	<p>INCIBE publishes security recommendations for use of cloud storage services</p> <p>INCIBE published a blog post outlining recommended security measures for the use of cloud storage services. The blog post acknowledges that the change in working practices due to the Covid-19 coronavirus pandemic has led to increased use of third party cloud storage services.</p> <p>The security recommendations include:</p> <ul style="list-style-type: none"> becoming familiar with the cloud storage provider's security and privacy policy to ensure it complies with the GDPR (and that information is stored on EU servers) and establish SLAs to set minimum compliance requirements; 	The blog post is available here (only in Spanish)	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • ensuring employees are aware of cloud service policy and what information can be stored where; • applying appropriate classification criteria to different types of information; • applying encryption techniques and limiting access to decryption keys; • implementing robust password and double factor authentication processes; • ensuring the third party cloud storage provider incorporates mechanisms that track access and modifications of stored documents; • ensuring the cloud storage solution incorporates malware protection and detection mechanisms; and • applying access controls on information stored in the cloud; • establishing back-up arrangements; and • applying secure erasure techniques to remove information that should no longer be stored and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			ensure cloud service provider policy addresses requirements.		
Spain	Spanish National Cybersecurity Institute (INCIBE)	28/4/20	<p>INCIBE publishes safety recommendations for using video calling apps</p> <p>INCIBE has published a blog post about secure use of video calling apps. The tips for organisations include the following:</p> <ul style="list-style-type: none"> • business users should consider commercial versions of videoconferencing apps and collaboration tools rather than basic free versions, and should verify that such tools comply with security, confidentiality and privacy requirements (including by studying the terms of use and privacy policy, and choosing the tool with a strong encryption mechanism for communications); • activate waiting rooms functionality and lock meetings once all participants have joined to prevent unauthorised persons joining the virtual meeting; • require a password to join the video call and protect access it by a strong password; 	The blog post is available here (only in Spanish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • set default functions to the safest options, such as deactivate the camera and the microphone—both video and microphone should be turned off when their use is not necessary. Participants should not share their desktop by default as this can lead to information leaks. The video reception should remain disabled by default and be used only when necessary; • when sharing the screen with other call participants, users should avoid sharing confidential information (e.g. username or device name, confidential documents, sensitive filenames); • if the meeting administrator intends to record the meeting, all participants must be notified about this. 		
Spain	Spanish National Cybersecurity Institute (INCIBE)	24/3/20	<p>INCIBE issues blog post on working remotely</p> <p>INCIBE has published a blog post about working remotely. The blog post highlights the importance of ensuring security guidelines are followed where employees work remotely, given the increased risk of cyber criminals accessing an organisation's network or employees using tools that are not permitted. The</p>	The blog post is available here (only in Spanish).	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>blog recommends organisations use a virtual private network to enable remote access to their systems and information in order to maintain confidentiality. The blog also highlights the importance of using corporate devices where possible, or ensuring personal devices are equipped with strong passwords.</p>		
Sweden	Swedish supervisory authority Datainspektionen	27/3/20	<p>Datainspektionen issues statement on the use of digital infection tracking tools</p> <p>The Datainspektionen issued a statement in relation to the use of digital infection tracking technology during the Covid-19 coronavirus pandemic.</p> <p>The statement confirms that, where personal data is processed (including in relation to public health measures targeting the Covid-19 coronavirus) adequate measures must be taken to minimise any intrusion or impact on the data subject. The Datainspektionen references the EDPB's recent statement on the processing of personal data in the context of the Covid-19 coronavirus (adopted on 19 March 2020, see above), and confirms that individual consent is likely required for processing geolocation data.</p>	The statement is available here (only in Swedish).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The Datainspektionen states that it will prioritise queries and consultation requests from developers of digital infection tracking technology where such technology processes personal data. However, the statement also confirms that the Datainspektionen shares supervisory responsibility over the use of location data in digital applications and mobile networks with the Swedish Post and Telecom Authority (the PTS), which monitors the electronic communications and postal sectors.		
Sweden	Swedish supervisory authority Datainspektionen	26/3/20	<p>Datainspektionen provides guidance on the Covid-19 coronavirus and the application of the GDPR</p> <p>The Datainspektionen updated the statement on application of the GDPR in relation to the Covid-19 coronavirus and FAQs that was provided initially on 13 March 2020. The statement emphasised that GDPR continues to apply to the processing of personal data (including sensitive personal data such as health data) in the context of the Covid-19 coronavirus pandemic and that taking necessary measures to prevent the spread of the virus must be balanced with the protection of employees' personal data.</p>	The statement is available here (only in Swedish).	Data protection-general guidance Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Employers must continue to comply with GDPR requirements and should, for example, avoid systematically gathering information about illnesses from employees.</p> <p>Information that a person is infected with the virus is considered personal health data, whereas information that someone has returned from a risk area, or is in quarantine (without giving further details on cause) is not considered personal health data. However, information that someone is quarantined under the Infectious Disease Control Act is likely to be personal health data.</p> <p>The statement also includes a list of FAQs; the answers have been expanded and clarified, including the following:</p> <ul style="list-style-type: none"> informing employees that a colleague might be infected by the Covid-19 coronavirus: as employer must take all necessary measures to prevent workers from being exposed to illness, it should be possible to inform the employees, if necessary, about infection without mentioning the name of the colleague. Only in 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>exceptional cases should it be necessary to specify who the victim is. If the employer considers that, for example, due to obligations in the labour law, it is absolutely necessary to reveal who has been infected, the employee in question shall be informed in advance, and only share information that is strictly necessary, accurate and not offensive to the employee concerned. In addition, the rules on professional secrecy and confidentiality might be applicable and should be taken into account;</p> <ul style="list-style-type: none"> informing that an employee works at home after being abroad/in a risk zone: it is possible to explain internally that the employee works at home but the Datainspektionen recommends not stating the reason. When informing people outside the organisation, the employer should carefully consider who needs to receive this information and not specify the reason, and communicate this information to third parties after consultation with the employee; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> collecting contact information for next of kin of employees: the employer may process contact information of employee's close relatives for the purposes of contacting them in case of accident or illness during working hours on the basis of legitimate interest (after performing a balancing test); measuring employees' body temperature: this is a significant invasion of privacy, but assessing employers' right to carry out checks and the obligation of workers to undergo the checks are mainly governed by labour law requirements, If an employer chooses to register personal data from the health checks, for example in an IT-based visitor system, that processing is covered by the GDPR and registration of this personal data is normally not permitted. 		
Switzerland	Swiss Federal Data Protection and Information Commissioner (FDPIC)	21/4/20	<p>FDPIC publishes assessments of contact tracing mobile app</p> <p>The FDPIC comments on the process of assessment of a "Covid proximity tracing app".</p>	The assessment is available here (in German).	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Following previous assessment by the École Polytechnique Fédérale de Lausanne (EPFL) on 21 March of the project for a "Covid proximity tracing app" (where it was considered that data protection had been taken into account due to voluntary participation and use of temporary identifiers for example), the EDÖB Corona Task Force carried out an assessment of the app on 2 April, which contacted vulnerable people through a centralised server.</p> <p>Subsequent development of the project, now termed DP-3T, employs a decentralised approach where anonymous keys are used and data retained locally. Whilst advantages of centralised approach are recognised, the decentralised version is preferred for data protection reasons, as noted during an assessment of 17 April.</p> <p>On 21 April the FDPIC noted that the EDÖB is examining the data protection aspects of the system architecture of the "DP-3T" model and requires proof of sufficient legal basis.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Switzerland	Swiss Federal Data Protection and Information Commissioner (FDPIIC)	9/4/20	<p>FDPIIC provides guidance on audio and video conference security</p> <p>The FDPIIC issued guidance on the maintenance of data security when attending virtual meetings given individuals and companies are increasingly looking for digital alternatives to communications during the pandemic.</p> <p>The guidance highlighted the importance of keeping an eye on data protection and information security issues when choosing the software used. In addition the FDPIIC emphasised the importance of:</p> <ul style="list-style-type: none"> ensuring solutions currently used can be used as safely as possible, even on a temporary basis during this extraordinary situation; and ensuring the services and products are reassessed, with a risk analysis being carried out based upon data protection criteria. <p>The factsheet recommendations include:</p> <ul style="list-style-type: none"> using one time meeting IDs, locking meetings, not sharing meeting IDs publicly and applying a password; 	<p>The press release is available here.</p> <p>The factsheet here. (both in German)</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • identifying attendees and announce recording; • beware of phishing and verifying meeting invitations from unknown sources; • taking care to manage webcam use and covering when not required, blurring backgrounds and limiting screen sharing to necessary information; • considering reputation of provider, reviewing privacy policy of providers including their approach to sharing meeting metadata and hosting and transferring data outside Switzerland and the EEA, encryption of data and physical security data centres, security functions in application; • configuring access settings; • setting use regulations and providing guidance to employees; • providing information regarding recordings of employees as required by law. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Switzerland	Swiss Federal Data Protection and Information Commissioner (FDPIC)	3/4/20	<p>FDPIC concludes that processing of anonymised telecom data by the Federal Office of Public Health to combat the Covid-19 Coronavirus is permitted under data protection law</p> <p>The FDPIC issued a statement clarifying that processing of telecom data provided by the telecom company Swisscom to the Federal Office of Public Health (FOPH) is lawful. The FDPIC requested earlier Swisscom to provide additional information on the processing and concluded that only anonymised data are accessed by the FOPH. To address public concerns about the consequences to privacy and protection of their personal data, the FDPIC requested Swisscom to publish information on the underlying data processing.</p> <p>According to the statement of the FDPIC, Swisscom processes anonymised statistical data on its Mobility Insights Platform (MIP) on basis of aggregated mobility data in order to evaluate mobility behaviour of individuals in Switzerland. The FOPH is provided with visualised data with an eight-hour delay to show the gatherings of large groups of individuals and assess the social distancing measures to combat the pandemic. This includes the time-lapse images</p>	The notices of FDPIC are available here (in German).	Data processing- location data Data processing- public authorities

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>representing aggregated data when there are more than 20 Swisscom mobile phone users are present in an area of 100 by 100 metres.</p> <p>The FDPIC clarifies:</p> <ul style="list-style-type: none"> • the location data of the users are pseudonymised (hashed) by Swisscom at the earliest possible stage and subsequently aggregated; • the FOPH receives only statistical information and data visualisations in the MIP, but not actual or pseudonymised user data; • the results (location data) accessible by the FOPH are aggregated and sufficiently anonymised. <p>Although data processing by Swisscom and the transfer of anonymous data to the FOPH are permitted under data protection law, the FDPIC noted that Swisscom and FOPH were not sufficiently transparent about data processing and data sharing. Following the FDPIC request, Swisscom published the FAQs regarding the use of MIP platform by the FOPH.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Switzerland	Swiss Federal Data Protection and Information Commissioner (FDPIIC)	17/3/20	<p>FDPIIC publishes guidance on data protection framework in relation to the Covid-19 coronavirus</p> <p>The FDPIIC issued guidance on the processing of personal data in relation to the Covid-19 coronavirus pandemic.</p> <p>The guidance covers data processing by healthcare institutions and private organisations. The guidance highlights that private organisations must follow the principles in Section 4 of the Federal Data Protection Act (FDPA) when handling personal data during the Covid-19 coronavirus outbreak, including the following:</p> <ul style="list-style-type: none"> health data are afforded special protection and, as a matter of principle, may not be obtained by private parties against the will of the individuals; processing of health data by private parties must be related to specific purpose and proportionate, meaning that collected data must be necessary and suitable for preventing further infections and must not go beyond what is necessary to achieve this purpose; 	The guidance is available here .	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-public authorities</p> <p>Data processing-health status</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • wherever possible, appropriate data on flu symptoms such as fever should be collected and passed on by the individuals themselves; • collection and further processing of health data by private third parties must be disclosed to the data subjects, including what data is collected, for which purpose and for which period. <p>The guidance also clarifies that any processing of personal data of employees or visitors in relation to prevention of Covid-19 coronavirus infection should be strictly limited to that purpose and proportionate. Personal data collected should be deleted when the pandemic threat ceases to exist. This applies to any processing of personal data by private individuals in connection with operational and organisational measures to prevent Covid-19 coronavirus infection, such as scanning bodily temperatures of visitors or employees entering their premises for the purpose of preventing infection.</p> <p>FDPIC notes that it considers answering extensive questionnaires about the health status to non-medical personnel as inappropriate and disproportionate.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Any intended use of digital methods for the collection and analysis of data on mobility and proximity of individuals must be proportionate to the purpose of preventing infection. This is only the case when these methods are epidemiologically justified and are proven to be an effective instrument for containing the pandemic in its current stage in order to justify any intervention with personal rights.</p>		
Switzerland	Reporting and Analysis Centre for Information Assurance (MELANI)	14/3/20	<p>Swiss MELANI warns about cybercrime attacks using Covid-19 coronavirus emails to spread malware</p> <p>MELANI, an organisation coordinating security of ICT systems and protection of critical national infrastructures in Switzerland, issued a warning about emails that pretend to be sent from the Federal Office of Public Health sent in relation to the Covid-19 coronavirus but instead attempt to spread malware called "AgentTesla". The malware allows the attackers to gain remote access to the computer and obtain passwords. MELANI urges the deletion of such emails immediately, without opening attachments or clicking on any hyperlinks in these emails. If the attachment was opened or a link clicked, MELANI recommends immediately turning off the computer,</p>	The press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			promptly changing passwords and contacting a specialist support service.		
UK [Updated as at 14 May 2020]	UK Department of Health and Social Care (DHSC)	4/5/20	<p>UK Department of Health and Social Care announces contact-tracing app trial</p> <p>The DHSC launched a trial of a contact tracing app developed by NHSX in the Isle of Wight, available for download from 5 May 2020.</p> <p>The app is intended to track and trace individuals that are potentially infected to minimise the spread of the Covid-19 coronavirus.</p> <p>The press release highlights:</p> <ul style="list-style-type: none"> • the methodology used (Bluetooth low energy technology); • the purpose of the app (for NHS care, management, evaluation, and research); • involvement of the UK NCSC to advise on best practice through development; and • prioritisation of privacy and security of users. 	The press release is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
UK	UK supervisory authority (ICO)	12/5/20	<p>ICO issues guidance for employers on workplace testing</p> <p>The guidance takes the form of FAQs and was issued at a time when the UK Government updated guidance with regards to working practices and encouraged more individuals back to work. The UK Government guidance for employers dated 11 May did not otherwise address temperature testing. However, as the ICO notes, the approach of the UK Government and other devolved nations to returning to work (amongst other things) differs. Therefore, consideration of the Government guidance such as the 11 May guidance for employers will likely be helpful alongside the ICO temperature testing guidance.</p> <p>The guidance addresses the following:</p> <ul style="list-style-type: none"> • Carrying out tests to check whether staff have Covid-19 coronavirus symptoms or the virus <ul style="list-style-type: none"> ○ Data protection laws should be taken in to account and personal data handled lawfully, fairly and transparently. 	The guidance is available here .	Data processing-employment Data processing-health status

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ Special category data such as health data should be even more carefully protected. ● The lawful basis for testing employees <ul style="list-style-type: none"> ○ For public authorities carrying out their function, public task is likely to be applicable. ○ For other public or private employers, legitimate interests is considered likely to be appropriate, but each organisation should make its own assessment. ○ Processing of health data requires identification of an Article 9 condition, and it will be the employment condition Article 9(2)(b), along with Schedule 1 condition 1 of the DPA 2018. This applies due to their employer health and safety obligations. The ICO considers that this condition will cover most of what employers need to do, as long as they are not collecting or sharing irrelevant or unnecessary data. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Demonstration that testing approach is compliant with data protection law <ul style="list-style-type: none"> ○ Use the accountability principle. Demonstrate compliance e.g. through additional recording keeping when processing sensitive data or through regularly reviewed and updated data protection impact assessment (DPIA). ○ A DPIA regarding health testing should focus on the new areas of risk and set out activity proposed; data protection risks; whether the activity is necessary and proportionate; mitigating actions; and a plan or confirmation that mitigation has been effective. • Data minimisation <ul style="list-style-type: none"> ○ Limit data to that necessary for the purpose, especially special category data. Demonstrate the reason for testing individuals or obtaining the results from tests. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ Ensure data is adequate and accurate, e.g. reflecting change in health status over time. ● Retaining lists of positive or symptomatic employees <ul style="list-style-type: none"> ○ Ensure use of the specific employee health data is actually necessary and relevant for purpose. ○ Ensure data processing is secure, and consider any duty of confidentiality owed to employees. ○ Ensure that lists do not result in any unfair/harmful treatment of employees for example, by avoiding inaccurate information and acknowledging changing health status. It is not fair to use, or retain, information collected about the number of staff who have reported symptoms for purposes they would not reasonably expect. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none">• Information for staff<ul style="list-style-type: none">○ Be transparent e.g. clear, open and honest with employees about how and why the organisation wishes to use the personal data; what personal data is required; retention periods; and who you will share it with. Offer opportunity to discuss.○ Use clear accessible privacy information though the ICO acknowledges that there might be challenges in providing detailed information due to the impact of the Covid-19 coronavirus.• Sharing positive test results.<ul style="list-style-type: none">○ Keep staff informed about potential or confirmed cases but avoid naming individual if possible, and do not provide more information than is necessary.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Exercise of information rights <ul style="list-style-type: none"> ○ Individuals need to understand what personal data is held and how it's used in order to exercise rights. ○ It should be easy to exercise rights with processes or systems in place to assist, e.g. a secure portal. • Disclosure of existing test results <ul style="list-style-type: none"> ○ Even if voluntarily provided, due regard must be given to the security of that data and any duty of confidentiality owed to those individuals who have provided test results. ○ Do not collect or share irrelevant or excessive data to authorities if this is not required. • Temperature checks or thermal cameras <ul style="list-style-type: none"> ○ More intrusive technologies, especially for capturing health information, require specific thought as to the purpose and context of use. Monitoring must be necessary and proportionate 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and in keeping with reasonable expectations.</p> <ul style="list-style-type: none"> The ICO has provided an updated Surveillance Camera Commissioner DPIA template, specific to surveillance systems but intended to assist thinking before use of thermal cameras or other surveillance. 		
UK	UK supervisory authority (ICO)	7/5/20	<p>ICO announces a pause on investigation into adtech industry</p> <p>The ICO has confirmed that it remains concerned about privacy issues in connection with real time bidding and the adtech industry. However, in order to avoid undue pressure on any industry during the Covid-19 coronavirus pandemic the ICO will restart investigations at a more appropriate time.</p>	The press release is available here .	Data protection-regulator approach
UK	UK supervisory authority (ICO)	7/5/20	<p>ICO issues a statement in response to media enquiries about the Data Protection Impact Assessment for the NHSX's Isle of Wight trial of contact tracing app</p> <p>Despite there being no legal obligation to do so, NHSX has asked the ICO to review informally its DPIA for the Isle of Wight trial of the contact tracing</p>	The statement is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			app. The statement simply confirms that the ICO is reviewing the same and will provide its comments as quickly as possible so that they can be usefully included in the learnings from the trial.		
UK	UK supervisory authority (ICO)	5/5/20	<p>ICO publishes a blog setting out new priorities for UK data protection during the Covid-19 coronavirus crisis and beyond</p> <p>In her blog, Elizabeth Denham referenced the ICO's 15 April approach to enforcement document (see further below) before acknowledging the ICO's role in enabling innovation whilst protecting the privacy of citizens. In monitoring trends, complaints and requests for support the ICO has determined that there are certain areas where the ICO's focus can have the greatest impact, specifically:</p> <ul style="list-style-type: none"> • protecting the public interest, focusing on information rights issues likely to cause most harm to people and business; • enabling data sharing, ensuring responsible sharing of data for the public good and responding to risk; 	<p>The Blog is available here.</p> <p>A related infographic is available here.</p>	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • monitoring intrusive and disruptive technology, protecting privacy whilst enabling innovation. <p>The blog specifies 6 priority areas for the coming months:</p> <ul style="list-style-type: none"> • protecting vulnerable citizens (responding to privacy and information rights risks, issues and opportunities through the crisis, taking action against those using/ obtaining personal data unlawfully or inappropriately during the crisis); • supporting economic growth and digitalisation (providing information, support and practical tools for businesses to enable safe service offerings when sharing personal data or developing AI); • shaping proportionate surveillance (including contact tracing, testing and other emerging surveillance issues); • enabling good practice in AI (shaping the development and use of AI in response to Covid-19 coronavirus to ensure privacy considerations are engineered into the use); 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> enabling transparency (supporting transparency about decisions taken that affect citizens); maintaining business continuity at the ICO (new ways of working in preparation for recovery). 		
UK	UK supervisory authority (ICO)	4/5/20	<p>ICO publishes a paper setting expectations on how Covid-19 coronavirus contact-tracing apps may be developed in line with the principles of Privacy by Design and Privacy by Default</p> <p>This ICO paper was provided to the Human Rights Joint Committee in advance of the appearance of Information Commissioner, Elizabeth Denham, and Executive Director of Technology and Innovation, Simon McDougall, before that Committee on 4 May 2020. This session was held to further discuss the UK Government's proposed contact tracing app.</p> <p>The paper is intended to assist technical design teams and to support ongoing discussions between the ICO and NHSX in the development of contact tracing apps.</p> <p>The paper considers that a data protection impact assessment must be carried out before app</p>	<p>The press release and access to Human Rights Committee session recording is available here.</p> <p>The Paper is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>implementation (processing is likely to result in a high risk to the rights and freedoms of individuals) and should go through iteration over time to reflect the app's functionality/scope, roadmaps updates and releases. Consideration should be given to triggers for refresh.</p> <p>The paper sets out ten principles to follow throughout the development and app life cycle, with testing against the same:</p> <ul style="list-style-type: none"> • Be transparent about: <ul style="list-style-type: none"> ○ the purpose of the app (including if it is likely to expand, considering necessity/proportionality of processing, considering all parties and provision of information within and outside app); ○ the design choices (use least privacy intrusive approach); and ○ the benefits (for all parties, being clear on managing tensions, and how solution addresses each in line with data protection requirements); 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Minimise personal data collection. • Protect users (using regularly renewed pseudonyms to reduce risk of re-identification and tracking) and give them control (to exercise rights through the app and control during onboarding and use); • Minimise and explain data retention and give users control over the same where appropriate, and avoiding gathering, augmenting and correlating user data without express permission; • Securely process data, using cryptographic/security techniques at rest and in transit to server/other apps. Confidentiality, integrity and availability should be engineered into services; • Ensure users can opt in/out without consequence and functions de-coupled; and • Strengthen privacy rather than weaken it (e.g. don't introduce additional risks such as requiring phone unlock or location identified). 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The paper goes on to outline best practices recommendations for contact-tracing apps during the various phases of development and use including, amongst other things:</p> <p>Scope, requirements and design:</p> <ul style="list-style-type: none"> • Be transparent and articulate benefits and objectives to users of data in an understandable way. • Exclude further processing for purposes unrelated to the primary aim and explain how data collection is minimised to address only those purposes. • Where additional functionality is developed re-assess privacy implications, describe and explain product roadmaps by reference to privacy impact and control measures and decouple functionality. • Consider legal basis to process personal data. • Consider separating information storage and access to user devices (e.g. exchange of proximity data and receipt of notifications) that is strictly necessary from that which is not-e- 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Privacy consent requirements apply in the latter case.</p> <ul style="list-style-type: none"> • Decouple functionality, assess processing and necessity, proportionality and lawful basis for each stage, put in place technical and policy is controls and document. • Open source code to scrutiny. • Consider the most appropriate design from a user perspective-decentralised approach more easily allows best practice compliance with data minimisation principle-consider how to use this model and how to move to that model in due course. <p>Development, deployment, onboarding and operation:</p> <ul style="list-style-type: none"> • Adopt a user-centric design approach, testing for different user needs and build technical and policy controls to ensure fair treatment. • Do not track location, directly identify users or process other device information (device IDs, call logs, IP addresses etc). 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Consider interoperability for use outside the UK (with associated controls to avoid data sharing risk). • Understand and comply with requirements of software components (APIs, SDK, frameworks, coding libraries etc) and avoid collection of data by third parties for other purposes. • Store information on device and only use backend infrastructure to collect personal data when strictly necessary for the function provided. • Consider data retention controls for storage of data locally and centrally, with retention periods proportionate and based on scientific/epidemiological evidence and for the duration of the crisis. • Use regularly refreshed pseudonyms, ideally generated on device. • Use of anonymised data (e.g. for research) should be documented with measure to avoid 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>re-identification. Assess research in the public interest with ICO and carry out a DPIA.</p> <ul style="list-style-type: none"> Backend infrastructure should process minimum amount of personal data, only collecting identifiers after voluntary user action, limiting use of identifiers for the time needed to inform other users and not attempting to identify individuals. Server logs should not contain identifiers. Backend infrastructure and transmission to the same should be secured with state of the art technology and authentication used with security testing in place. Access restrictions should be applied and data exchange limited to those supporting notification delivery. Risk of self-reporting false positives should be addressed and passwords used for submission. Processes to avoid incorrect matching of identifiers should be developed, audited and regularly reviewed. Users should receive clear information about the app, data processed, parties involved, and be able to access GDPR rights. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Decommissioning:</p> <ul style="list-style-type: none">• Consider from the outset, both for general and individual decommissioning.• Consider whether specific processes are necessary to dismantle or whether it will dismantle itself once use declines and how to inform users.• Address steps necessary to erase or anonymise data once the app is no longer relevant.• Consider how to ensure decommissioning is auditable and verifiable, including by the ICO.• Consider future use of personal data/models for research purposes, ensuring in compliance with data protection law and with appropriate safeguards in place.• Allow for lessons learned process.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
UK	UK supervisory authority (ICO)	24/4/20	<p>ICO issues statement on the NHS tracing app, developed to combat the Covid-19 coronavirus</p> <p>The ICO has responded to an NHSX Blog regarding the contact tracing app developed to assist in the fight against the Covid-10 coronavirus.</p> <p>The blog describes the nature of the contact tracing app and the process to launch in the coming weeks.</p> <p>The app:</p> <ul style="list-style-type: none"> • will be used in conjunction with other practical and health measures; • alerts people who may have been exposed to the Covid-19 coronavirus so they can take action to protect themselves and others; • uses Bluetooth Low Energy to log the distance between an individual's phone and others nearby; • stores an anonymous record securely on the mobile device; • enables an unwell individual (with Covid-19 coronavirus symptoms) to choose to allow the app to inform the NHS which, subject to 	<p>The statement is available here.</p> <p>The NHSX Blog is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>sophisticated risk analysis, will trigger an anonymous alert to those other app users with whom the infected individual came into significant contact over the previous few days; and</p> <ul style="list-style-type: none"> provides advice regarding next steps to take if infected. <p>In future releases of the app, people will be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends. This is described in voluntary terms but with tones of encouragement-highlighting the beneficial role such information will fulfil.</p> <p>The blog goes on to describe data usage in more detail:</p> <ul style="list-style-type: none"> confirming patient confidentiality as a priority and the intention to comply with the Data Protection Act. Transparency is held out as key for individuals and the broader community, with a proposal to publish security and privacy designs along with source code; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • flagging the app's development with privacy by design being implemented • noting that data use will only ever be for NHS care, management, evaluation and research, though it is unclear how long that research may last for; • highlighting steps taken to avoid ethical or legal failures, including consultation with the ICO, the National Data Guardian's Panel and the Centre for Data Ethics and Innovation, as well as with representatives from Understanding Patient Data and volunteers who provided a patient and public perspective. NHSX has also established an ethics advisory board for the app, as well as engaging an independent assurance board (which includes experts in mobile apps, data governance and clinical safety) to ensure that the app will be stable, resilient, secure, performant, highly usable and above all effective in the fight against the Covid-19 coronavirus. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			In its statement, the ICO recognises the role that data can play as well as the need to act quickly. The ICO confirms that it has been working with NHSX to help them ensure a high level of transparency and governance.		
UK	UK supervisory authority (ICO)	17/4/20	<p>ICO posts a blog of questions to aid privacy considerations for users of new technologies in the context of Covid-19 coronavirus</p> <p>The Information Commissioner has posted a blog highlighting the advantages of new technology in combatting the Covid-19 coronavirus pandemic, such as contact tracing projects and location tracking but flagging the need to use such technology in a fair, proportionate and transparent way.</p> <p>The blog notes this as an international issue and following ICO analysis and discussions of commissioners, government representatives, privacy professionals and others it sets out a series of questions to consider when using new technologies. The aim is to ensure that the privacy implications are considered, and that public trust and social licence is not put at risk.</p>	The blog is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The questions are:</p> <ul style="list-style-type: none"> • Have you demonstrated how privacy is built in to the processor technology? <ul style="list-style-type: none"> ○ Organisations creating apps will need to account for privacy by design and default. ○ An initial privacy impact assessment that is then developed is a minimum requirement. • Is the planned collection and use of personal data necessary and proportionate? <ul style="list-style-type: none"> ○ The public need to know that thought is being given to finding the least privacy intrusive solutions. ○ This is especially important regarding "location data", some of which can be more exact than others. ○ Some projects may be able to rely on data that is pseudonymised or anonymised to reduce the risk of re-identification. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ Evidence and context should inform conversations on proportionality. ● What control do users have over their data? And can they exercise their rights? <ul style="list-style-type: none"> ○ App developers must provide clear information on how their information was being used, and their options for preventing processing where applicable. For instance, where contact tracing is being incorporated into a wider package of measures, this additional information would need to be clear. ● How much data needs to be gathered and processed centrally? <ul style="list-style-type: none"> ○ The starting point for contact tracing should be decentralised systems (e.g. on device) with associated security measures and information transfer. ● When in operation, what are the governance and accountability processes in your organisation for ongoing monitoring and evaluation of data processing – to ensure it 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>remains necessary and effective, and to ensure that the safeguards in place are still suitable?</p> <ul style="list-style-type: none"> • What happens when the processing is no longer necessary? • What consideration has been made to how data collection ends, and what happens to the data gathered? <p>The ICO references its opinion published on the Google/Apple joint work on contact tracing.</p>		
UK	UK supervisory authority (ICO)	15/4/20	<p>ICO publishes a blog advising on security of teleconferencing in the context of the Covid-19 coronavirus pandemic</p> <p>The ICO has published a short blog recognising the challenges of ensuring security of teleconferencing and remote business whilst maintaining convenience.</p> <p>It highlights the advice it can provide to employees on the topic generally and five key questions to ask:</p> <ul style="list-style-type: none"> • Have you checked the privacy and security settings? 	<p>The blog is available here.</p> <p>The Data Protection and Working from Home, What you need to Know collection is available here.</p> <p>The security checklist is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ Consider transparency of video conferencing technology and how users can control use of their data. ○ Advise employees, and make use of, privacy and security features to manage access to meetings such as through password control, timing restrictions, screen sharing limits, communication of invitation protocols. ● Are you aware of phishing risks? <ul style="list-style-type: none"> ○ Beware of phishing in the context of video features such as the "live chat feature" – don't click on links/attachments you were not expecting or from meeting attendees you do not recognise. ● Have you checked your organisation's policy? <ul style="list-style-type: none"> ○ Organisations should select a video conferencing platform that matches their policies and employees should check and use the same. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Have you ensured all software is up-to-date? <ul style="list-style-type: none"> ○ Apply regular software and browser updates. • Is this still the right tool for the job? <ul style="list-style-type: none"> ○ Re-visit and review your choice of video-conferencing tool after the Covid-19 coronavirus crisis when you have time and resources to do so to ensure it remains appropriate. <p>The blog is included alongside more general advice regarding working from home securely and bring-your-own-device arrangements, as well as a security checklist for employers which references the particular challenges of the Covid-19 coronavirus crisis.</p> <p>The security checklist itself notes that data protection law does not prevent employers from using IT solutions but time should be taken to ensure secure use. The checklist is intended as a support to identifying some of common IT vulnerabilities but is not a complete security assessment.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Issues for an employer to consider are set out:</p> <p><i>General principles</i></p> <p>Has the employer implemented clear remote working policies, procedures and guidance (including regarding password use), implemented the most up-to-date version of remote access solution and configured multi-factor authentication where possible.</p> <p><i>Bring your own device (BYOD)</i></p> <p>The checklist flags the ICO's comparison to help decide which is the best option for the organisation.</p> <p><i>Cloud storage</i></p> <p>Has the employer considered additional risks that can arise through cloud use such as avoiding publicly accessible cloud storage, applying access restrictions and security. The checklist also directs employers to guidance regarding cloud use and National Cyber Security Centre guidance on security within Software as a Service (SaaS).</p> <p><i>Remote desktop</i></p> <p>Has the employer limited remote access use as required, disabled default administrator accounts,</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>created specific privileged accounts and ensured account lockouts are in place.</p> <p>The checklist notes that long-term strategies such as VPN access are preferable to short-term fixes.</p> <p><i>Remote applications</i></p> <p>Remote application help prevent staff from using their own personal applications to process personal data but the checklist recommends checking admin tool access, shortcut usage and location of username and password information.</p> <p><i>Email</i></p> <p>Has the employer implemented the UK NCSC guidance on defending against phishing attacks, blocked forwarding rules and advised staff to use corporate email solutions in preference to their own.</p>		
UK	UK supervisory authority (ICO)	15/4/20	<p>ICO explains its approach to regulation during the Covid-19 coronavirus emergency</p> <p>The ICO's paper explains how the regulator will act proportionately, taking into account the economic impact of the crisis on organisations as well as on their staff and operational capacity. It also notes that it</p>	<p>The statement is available here.</p> <p>The paper is available here.</p>	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>will take action against organisations seeking to exploit the crisis. In particular it highlights that:</p> <ul style="list-style-type: none">• Organisations should continue to report personal data breaches, without undue delay and within 72 hours of becoming aware of the breach. It acknowledges that the current crisis may impact this and that it will assess breach reports, taking an appropriately empathetic and proportionate approach.• When conducting investigations, the ICO will act taking account of the public health emergency and seeking to understand the individual challenges faced by organisations, including the particular impact of the crisis on that organisation. This may mean less use of formal powers that require organisations to provide evidence and allowing longer periods to respond. The ICO expects to conduct fewer investigations, with a focus on serious non-compliance.• It will take a strong regulatory approach against any organisation breaching data protection laws to take advantage of the current crisis.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • Audit work has been stood down in recognition of the economic impact on organisations and the current travel and contact restrictions in force. • In deciding whether to take formal regulatory action, including issuing fines, the ICO will take into account whether the organisation's difficulties result from the crisis, and if it has plans to put things right at the end of the crisis. It may give organisations longer than usual to rectify any breaches that predate the crisis, where the crisis impacts the organisation's ability to take steps to put things right. • All formal regulatory action in connection with outstanding information request backlogs will be suspended. • Before issuing fines the ICO will take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces. • Enforcement may not be taken against organisations who fail to pay or renew their data protection fee, if they can evidence that this is specifically due to economic reasons linked to the 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>present situation, and provided that adequate assurances are provided by the organisation as to the timescale within which payment will be made.</p> <ul style="list-style-type: none"> The ICO will recognise that the reduction in organisations' resources could impact their ability to respond to Subject Access Requests, where they need to prioritise other work due to the current crisis and this will be taken into account when considering whether to impose any formal enforcement action. 		
UK	UK supervisory authority (ICO)	8/4/20	<p>ICO issues a statement outlining its readiness to exercise its enforcement powers in respect of organisations taking advantage</p> <p>The ICO's statement explains that, whilst the regulator is keen to support business and help them use personal data responsibly during the Covid-19 coronavirus crisis, it is ready to investigate and take action against those organisations that exploit the crisis.</p>	The statement is available here .	Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The ICO:</p> <ul style="list-style-type: none"> • flags an increase in complaints received, especially regarding nuisance calls and the fact that it is prioritising those cases; • calls out organisations setting up scams and contacting vulnerable people using nuisance calls, unsolicited emails, and spam texts; • highlights its ability to issue penalties under electronic marketing rules to company directors and their companies, with fines of up to £500,000; and • notes that it is working closely with Action Fraud, Trading Standards, law enforcement, and other relevant agencies, to continue to protect people, raise awareness, and stop criminals during this challenging period. 		
UK	UK supervisory authority (ICO)	28/3/20	<p>ICO issues a statement regarding its position on the use of mobile phone tracking data in the context of the Covid19 coronavirus crisis</p> <p>The ICO states that if location data is properly anonymised and aggregated, it does not fall under data protection law because no individual is identified.</p>	The statement is available here .	Data processing-location data

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>Therefore, privacy laws are not breached as long as the appropriate safeguards are in place.</p> <p>The statement clarifies that safety and security of the public remains the ICO's primary concern and that they will work to provide advice about data protection law.</p>		
UK	UK supervisory authority (ICO)	12/3/20 Further updated	<p>ICO issues statement on data protection law and Covid-19 coronavirus</p> <p>The ICO issued a statement clarifying that data protection and ePrivacy laws do not prevent Government, the NHS or any health professionals from sending public health messages to people. These authorities may use the latest technology to facilitate safe and swift consultations and diagnoses or require additional collection or sharing of personal data to protect public health.</p> <p>The ICO also issued guidance to controllers, where it takes a pragmatic approach to the enforcement of data protection requirements in light of the pandemic.</p> <p>As at 14 May 2020 the original link to guidance for controllers of 12 March 2020 is no longer available but the statement directs readers to a "Data protection and Coronavirus-what you need to know</p>	<p>The statement is available here.</p> <p>As at 14 May 2020 the original link to guidance for controllers of 12 March 2020 is no longer available but the statement directs readers here.</p> <p>The ICO Data Protection and Coronavirus information hub is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>page", setting out FAQs and linking to guidance for health and social care organisations and workplace testing guidance of 12 May 2020 as further covered above.</p> <p>The FAQs cover most of the issues addressed in the 12 March 2020 controller guidance, ie the ICO:</p> <ul style="list-style-type: none"> • confirmed that it will not penalise organisations for failure in meeting statutory deadlines due to diverting compliance resources to other areas of work in this extraordinary period; • clarified that organisations should keep staff informed about colleagues that have potentially contracted Covid-19 coronavirus infections but should refrain from naming individuals and providing more information than necessary; • notes that although it is unlikely that an organisation will have to share information with authorities about specific employees, data protection laws will not prevent it from sharing if necessary. <p>This set of FAQs no longer addresses whether it is reasonable to ask employees or visitors if they have</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>visited a particular country or experience Covid-19 coronavirus symptoms but the FAQs do:</p> <ul style="list-style-type: none"> • make further reference to the more developed enforcement approach of 15 April 2020 as described above; • highlight home working security advice, also described in more detail above; • note community group guidance; • address the provision of privacy notices and information about how organisations are processing personal data during the Covid-19 coronavirus pandemic, specifically the need for a privacy notice, information it should include and, if not already prepared, the expectation that a notice will be in place and updated as soon as reasonably practical; • discuss the approach to a personal data breach due to adaptations made during the Covid-19 coronavirus pandemic (several breaches involving email human error have occurred so staff communications and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>reference to working from home guidance to assist).</p> <ul style="list-style-type: none"> consider how to show that personal data processing during the pandemic is compliant, noting the accountability principle, the need for a DPIA if processing health information, suggested content and the need to keep under review. <p>The ICO has looked to consolidate its advice and resources on a dedicated information hub, covering the above, as well as a blog regarding data protection for community groups (looking to assist in the crisis), the ICO's approach to Freedom of Information, information for individuals about data protection, and details of the ICO's availability and hotline.</p>		
<p>UK</p>	<p>The UK National Cyber Security Centre (UK NCSC)</p> <p>The Cybersecurity and Infrastructure Security Agency (CISA)</p>	<p>5/5/20</p>	<p>The UK NCSC, the US CISA and DHS issue a joint warning of advanced persistent threat (APT) groups targeting healthcare bodies, pharmaceutical companies, and medical research organisations, among others</p> <p>The latest warning follows a joint advisory publication issued on 8 April regarding cyber criminal exploitation</p>	<p>The NCSC news report and alert are available here and here.</p> <p>The CISA press release is available here.</p>	<p>Cybersecurity and Information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
	The U.S. Department of Homeland Security (DHS)		<p>of the Covid-19 coronavirus outbreak for their own personal gain (see later in this overview).</p> <p>The current alert highlights ongoing activity by APT groups against organisations involved in both national and international Covid-19 coronavirus responses, in particular pharmaceutical companies, research organisations, and local government, targeting organisations to collect bulk personal information, intellectual property and intelligence that aligns with national priorities.</p> <p>The alert describes some of the methods APTs are using to target organisations. For example, ‘password spraying’ campaigns against healthcare bodies and medical research organisations (where the attacker tries a single and common password against many accounts before moving on to try a second password etc) and scanning external websites of targeted companies for vulnerabilities in unpatched software, taking advantage of vulnerabilities such as those in Virtual Private Network (VPN) products from certain vendors.</p>	<p>The CISA alert is available here.</p> <p>The joint advisory is available here.</p>	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The joint advisory report goes on to describe a number of mitigations including:</p> <ul style="list-style-type: none"> • updating Virtual Private Networks, network infrastructure devices, and devices being used to remotely access the work environment with the latest software patches and configurations; • using modern systems and software with better in-built security; • using multi-factor authentication to reduce the impact of passwords being compromised; • protecting the management interfaces of critical operating systems; • setting up security monitoring systems; and • reviewing and refreshing incident management processes. <p>The advisory directs reader to a number of existing guidance documents of both the UK NCSC and the US CISA.</p> <p>The alert states that the NCSC and CISA will continue to investigate activity linked to APT actors.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
UK	The UK National Cyber Security Centre (UK NCSC)	4/5/20	<p>The UK NCSC publishes a Technical Paper detailing to its support for the NHSX contact tracing app.</p> <p>The UK NCSC has stated that privacy and security of NHSX app users' data is a priority. Its Technical Paper, along with a Blog post, Explainer and Infographic explain the security behind the NHSX app, and how it will help in the fight against Covid-19 coronavirus whilst protecting people's privacy.</p> <p>The Technical Paper, amongst other things:</p> <ul style="list-style-type: none"> • describes how the app works and operates (including use of randomly generated identifiers, storage of contacts on device, voluntary transfer of data to the centralised server for analysis and subsequent notification to contacts), the system architecture and app lifecycle; • specifies security and privacy criteria including: <ul style="list-style-type: none"> ○ minimising collection of personal data; ○ obtaining active user consent for action involving collected data; 	<p>The press release is available here.</p> <p>The Technical Paper is available here.</p> <p>The Blog Post is available here.</p> <p>The Explainer is available here.</p> <p>The Infographic is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ not tracking users over time through Bluetooth transmission; ○ not enabling external observers to associate Bluetooth transmission with device-specific information (other than proximity inference); ○ not enabling submission of spoofed data; ○ not enabling recipients of a notification to determine which of the people they have been in contact with has shown symptoms ○ system tolerance to the actions of malicious users seeking to gain from a false self-diagnosis, to cause mass notification in a given area (e.g. trying to shut down a hospital), to cause panic through mass notification across the country (e.g. by a nation state actor); ○ not enable replay of a notification of proximity from the service to another user. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none">explains how the UK NCSC considers these criteria are met;describes re-identification risk and considers that at the time of writing, there is insufficient data used to attract any re-identification risk;highlights distinction between centralised and decentralised approach and risk with decentralised. <p>The Blog, amongst other things:</p> <ul style="list-style-type: none">covers many of the issues raised in the Technical Paper in a more accessible style;also discusses decentralised vs centralised approaches and privacy considerations;highlights re-identification risk;acknowledges use of the term anonymous in the blog is not intended to mean anonymous data as understood by the GDPR;encourages use of the app.		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The Explainer includes a number of FAQs that address the same topics, including how the app can be used and the data that is collected.		
UK	The UK National Cyber Security Centre (UK NCSC)	21/4/20 Updated 22/4/20 and 5/5/20	<p>UK NCSC publishes guidance for organisations on videoconferencing as part of a Cyber Aware campaign</p> <p>Whilst not specific to the Covid-19 coronavirus, the UK NCSC is mindful of the increased cybersecurity risk and has produced guidance for organisations (and individuals) holding online video conferences.</p> <p>The guidance forms part of the cross-governmental Cyber Aware campaign designed to promote behaviours that mitigate threats. The campaign encourages people to 'Stay home. Stay Connected. Stay Cyber Aware', and its top tips for staying secure online are to:</p> <ul style="list-style-type: none"> • turn on two-factor authentication for important accounts; • protect important accounts using a password of three random words; • create a separate password that is only used for an individual's main email account; 	<p>The press release is available here.</p> <p>The guidance is available here.</p> <p>The UK NCSC press releases regarding the SERS are available here and here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • update the software and apps on devices regularly (ideally set to 'automatically update'); • save your passwords in browser; • back up important data to avoid ransom risk. <p>The UK NCSC has also set up a scam-reporting service (Suspicious Email Reporting Service or SERS) for people to flag suspicious emails and for the UK NCSC to take down malicious content (noting that it had removed more than 2,000 online scams related to Covid-19 coronavirus in the last month).</p> <p>More than 80 malicious web campaigns were taken down after 5,000 suspicious emails were flagged to SERS for investigation, within a day of its launch. In just over two weeks the public has passed on more than 160,000 suspect emails, with more than 300 bogus sites taken down. The UK NCSC has shared some examples of those sites.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>In particular, the videoconferencing guidance addresses:</p> <ul style="list-style-type: none"> • how organisations should choose a video conferencing service; • how organisations deploy such a service; and • how organisations should aid employees to use such services securely. <p>When choosing a supplier organisations are encouraged to:</p> <ul style="list-style-type: none"> • examine existing providers-carrying out a new security risk assessment. The guidance highlights the advantages of working with BAU providers where staff are familiar with the applications, where systems will already be configured and integrated with audit and monitoring and should be compliant with data handling legislation; • carry out a risk analysis of any new service provider, which could include use of the UK NCSC SaaS security guidance, requesting independent assessment or audit, and 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>assessment of terms and conditions (such as how provider implements basic security controls, where data is held, and what they can do with it);</p> <ul style="list-style-type: none"> • follow the UK NCSC cloud security principles if video conferencing is required for more sensitive meetings (such as government, regulated industry sector and organisations with personal data) to determine needs; • consider additional features such as end-to end encryption; • consider location of data storage and whether data is routed through different jurisdictions. <p>When deploying video conferencing the guidance recommends:</p> <ul style="list-style-type: none"> • using company-wide defaults and controls balancing security and user needs; • setting up single-sign on, integrating use with existing corporate identities; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • configuring any password sign-on with the UK NCSC password guidance, including multifactor authentication; • applying least privilege role based access controls; • permitting authenticated users straight into a meeting, but requiring unauthenticated users to submit a passcode and holding in a waiting area until verified; • considering blocking video calls from outside the organisations that are not in user contact lists or are from unidentified or unauthenticated users; • considering use of in-conference features like screen and file sharing, messenger chats, call transcript and recordings, is this is appropriate in context and where data is stored; • configuring consistently across platforms accessing through devices configured as described in the UK NCSC's devices guidance; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • avoiding downloads of apps when joining calls; • considering exception to always-on VPN for video conferencing to improve performance as long as it uses well-configured encryption and authentication; • avoiding reconfiguring and installing apps to enable use of other organisations video conferencing service (access via web browsers). <p>When communicating with staff guidance recommends:</p> <ul style="list-style-type: none"> • providing clear user guidance; • asking users to test pre-real meetings so they can be familiar with systems such as muting and turning off cameras to aid security; • asking users to treat the details explaining how to join the meeting as if it is as sensitive as the meeting itself and to only share passwords with participants; • considering blurring their background or using a background image (if this is a feature is 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>available) to improve personal privacy when working from a home;</p> <ul style="list-style-type: none"> informing how to check the webcam is operating or offer options to physically block the same; informing how to check whether the call is being recorded; and ensuring users verify participants on the call and remove those that are not identified. 		
<p>UK</p>	<p>The UK National Cyber Security Centre (UK NCSC)</p> <p>The Cybersecurity and Infrastructure Security Agency (US CISA)</p> <p>The US Department of Homeland Security (DHS),</p>	<p>8/4/20</p>	<p>UK NCSC and the US CISA publish a joint advisory on malicious cyber activity exploiting the Covid-19 coronavirus pandemic</p> <p>The UK NCSC and the US CISA published a joint advisory with an overview of malicious cyber activity related to the Covid-19 coronavirus pandemic. The advisory provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups, includes a non-exhaustive list of indicators of compromise for detection of attacks and practical advice on mitigating related risks.</p>	<p>The press statement of the US CISA is available here.</p> <p>The press statement of the UK NCSC is available here.</p> <p>The advisory is available here.</p>	<p>Cybersecurity and information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The advisory notes that APT groups and cybercriminals are actively using the pandemic for commercial gain, deploying various threats, including:</p> <ul style="list-style-type: none">• phishing and malware distribution, while using the subject of coronavirus or Covid-19 as a lure;• registration of new domain names containing wording related to Covid-19 or coronavirus; and• attacks against newly deployed remote access and teleworking infrastructure, by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. <p>Recommendations for organisations include:</p> <ul style="list-style-type: none">• using passwords or "waiting room" features for online meetings to control admittance of participants;• managing screen sharing options when using communication platforms for online meetings;		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • ensuring teleworking policies address physical and information security requirements; • planning for successful phishing attacks; and • educating employees in identifying and reporting suspected phishing emails. <p>The advisory also identifies key online resources published by the UK NCSC and US CISA in relation to mitigating risk online, including:</p> <ul style="list-style-type: none"> • CISA guidance for defending against Covid-19 cyber scams; • CISA insights on risk management for Covid-19 with guidance for executives regarding physical, supply chain, and cybersecurity issues; • NCSC guidance to help spot, understand, and deal with suspicious messages and emails, guidance on phishing for organisations and cybersecurity professionals, and other materials. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
UK	National Cyber Security Centre (UK NCSC)	17/3/20	<p>UK NCSC publishes guidance on Covid-19 coronavirus cybersecurity risks of working from home</p> <p>The UK NCSC published guidance for companies on managing and mitigating additional cybersecurity risk arising from home working in the context of the Covid-19 coronavirus, particularly due to increased phishing attacks and increased risk of theft.</p> <p>Recommendations include:</p> <ul style="list-style-type: none"> • setting strong passwords and implementing multi-factor authentication when establishing user accounts; • employee education regarding new software and reporting issues; • data encryption; • use of antivirus tools, especially when using removable media; • using the VPN and security patching of the existing VPN. 	<p>The press release is available here.</p> <p>The guidance is available here.</p>	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			The guidance also advises on how to spot a phishing attack and some actions to take if you have engaged with one.		
MIDDLE EAST					
Israel	The Supreme Court in Jerusalem (SCJ)	26/4/20	<p>SCJ decision prohibits intelligence services from tracking of mobile data in the Covid-19 context unless new laws are passed</p> <p>The SCJ, the highest court of Israel, has ruled that the Israeli General Security Service (GSS) is no longer permitted to process the "technological data" (including telephone location data) of citizens based on the temporary emergency powers granted by the government to GSS in March 2020 under the national security law provisions, prompted by the Covid-19 coronavirus pandemic.</p> <p>The SCJ notes that if the state seeks to continue to use the tracing and monitoring activities of GSS, it must act to anchor such powers in primary legislation passed by the parliament. The SCJ determined that in this case the validity of the emergency decree may be extended for an additional short period (not exceeding</p>	The SCJ decision is available here (in Hebrew).	<p>Mobile apps and new technology</p> <p>Data processing-public authorities</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>a few weeks), only to allow the completion of the legislative process in this respect.</p> <p>The SCJ emphasised that it considers tracking of individuals without their permission to be a serious violation of Israeli citizens' right to privacy and a breach of the Israeli privacy law. The court also stated that any use of contact tracing mobile apps should abide by data protection principles.</p>		
Israel	Privacy Protection Authority (PPA)	22/4/20	<p>PPA issues guidance on the use of social ranking technology, including in the context of the Covid-19 coronavirus pandemic</p> <p>The PPA has published a review into the privacy impacts of the use of "social ranking" technology in Israel. In particular, the PPA examines social ranking as a potential tool in combatting the Covid-19 coronavirus pandemic.</p> <p>The review document explains that social ranking is the general term used for a systematic and on-going rating system of individuals. It involves collecting information about individuals and cross-linking this with other information to issue a "score" that compares a person to others.</p>	<p>The review is available here (in Hebrew).</p> <p>The press release is available here (in Hebrew).</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>In the context of Covid-19 coronavirus, a social ranking system based on artificial intelligence may be used to assess an individual's likelihood of contracting the disease based on factors such as their location and medical history. The additional variables used could include age, gender and workplace.</p> <p>The PPA concludes that the use of social ranking technology systems, including for dealing with the pandemic, will necessarily seriously violate an individual's right to privacy and therefore should be viewed as an exceptional measure. The PPA emphasises that social ranking should be avoided as much as possible and used only when no less intrusive alternatives are available. This solution can only be used subject to principles of proportionality, transparency and purpose limitation.</p> <p>The PPA also notes that storing personal data of everyone in Israel in one database could increase data breach risks.</p> <p>The guidance sets out conditions that the PPA believes should be met for the use of social ranking to prevent the spread of Covid-19 coronavirus. This includes the relevant public authority acting only in accordance with the powers vested in it by law,</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			obtaining the data subject's consent and adhering to privacy by design principles.		
Israel	Privacy Protection Authority (PPA)	23/3/20	<p>Privacy Protection Authority publishes general guidance on privacy and cybersecurity issues relating to the Covid-19 coronavirus</p> <p>The PPA has published guidance on the privacy implications of the measures that the Israeli government is taking to prevent the spread of the Covid-19 coronavirus, which include emergency regulations.</p> <p>The PPA confirms that the Israeli Privacy Protection Act 1981 (the 1981 Act) should not impede health services and other similar organisations processing personal information as required in the current emergency, and accepts that there is a public interest in the situation.</p> <p>The guidance emphasises the consent requirements under the 1981 Act and that breach of the act is a civil offence. The PPA however also notes that a violation of privacy can be considered justified in certain circumstances, such as the existence of an emergency situation, but in such circumstances the principles of data protection law must still be adhered</p>	The guidance is available here (only in Hebrew).	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Cybersecurity and information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>to. The guidance sets out these principles, including using the information only for the purpose for which it was collected and deleting the information where it is no longer required. It also reiterates that data subjects have rights including the correction, rectification or deletion of their personal data.</p> <p>The guidance also sets out responses to certain key employment questions arising from the Covid-19 coronavirus. Amongst other issues, the PPA clarifies that employers are allowed to tell employees that a colleague has contracted the virus (as long this is in good faith and the privacy laws are adhered to) and sets out requirements for transferring information between organisations.</p> <p>The guidance further considers the privacy aspects of remote working and distance learning and promotes the use of cybersecurity measures such as strong passwords, two-step authentication and awareness of cyber threats.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
Israel	Ministry of Health	22/3/20	<p>Ministry of Health launches app identifying user exposure to Covid-19 Coronavirus</p> <p>The Ministry of Health has announced the launch of a national app identifying user exposure to confirmed cases of Covid-19 coronavirus in Israel. The app is described as a technology device designed to inform individuals quickly and accurately whether they have been in contact with anyone infected with the Covid-19 coronavirus, with the intention of stopping the spread. The app gives the user an alert when they have been exposed to a verified patient (based on location and time). The Ministry of Health emphasises that the app retains location information solely on the user's device and combines this personal information with the Ministry's own records, which are sent to and updated on the app, to create the alert.</p>	The announcement is available here (only in Hebrew).	Mobile apps and new technology
Israel	Privacy Protection Authority (PPA)	19/3/20	<p>Privacy Protection Authority publishes Q&As on the impact of the Covid-19 coronavirus</p> <p>The PPA has made available to the public its responses to key queries from businesses in various sectors of the economy. In particular:</p> <ul style="list-style-type: none"> • In response to a query from the Israeli Railways, the PPA understands that the Ministry of Transport has asked public transport operators to 	The Q&A are available here (only available in Hebrew).	Data protection-general guidance Data protection-regulator approach

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>provide passengers with certain travel information over the telephone on request. The PPA sets out the privacy measures that should be put in place for this to be implemented, such as providing the information only for the purposes of preventing the spread of Covid-19 coronavirus.</p> <ul style="list-style-type: none"> In light of the exclusion of escorts and family members from hospital, following a query regarding the provision of medical information by telephone, the PPA sets out the steps that could be taken by hospitals to ensure that a high privacy standard is maintained without increasing the burden on medical staff (e.g. use of a code word and identification procedures for those who use that word). <p>The PPA also confirms that it has set up a hotline to answer queries from the general public regarding privacy.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
United Arab Emirates (Abu Dhabi)	Office of Data Protection (ODP) of the Abu Dhabi Global Market (ADGM)	20/3/20	<p>Office of Data Protection of Abu Dhabi Global Markets issues FAQ document addressing issues surrounding the Covid-19 coronavirus</p> <p>The ODP issued its responses to a set of frequently asked questions on topics relating to the Covid-19 coronavirus and data protection.</p> <p>The document sets out how the ADGM's Data Protection Regulations 2015 (the DPR 2015) will apply to situations arising from the Covid-19 coronavirus. It clarifies that the data controllers should comply with their responsibilities under DPR 2015, but that personal data can still be processed in the case of an emergency as long as this is done fairly, lawfully and securely, and is adequate, relevant, and appropriate in relation to the purposes of that processing.</p> <p>However, the ODP will take a pragmatic approach when assessing whether any processing of data in this context is non-compliant with the legislation and will consider any mitigating circumstances that apply. In particular, the ODP understands that there may be delays for data controllers responding to subject access requests at this time.</p>	The FAQs are available here .	<p>Data protection-general guidance</p> <p>Data processing-employment</p> <p>Data processing-health status</p> <p>Data protection-regulator approach</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The document considers several issues around the processing of health data by employers in the context of the Covid-19 coronavirus. It reiterates that a data controller has a duty to ensure the health and safety of its employees, but that restrictions apply to the collection and sharing of health data under the DPR 2015.</p>		
<p>United Arab Emirates (Dubai)</p>	<p>Dubai International Financial Centre (DIFC)</p>	<p>26/4/20</p>	<p>DIFC introduces legislation seeking to limit the impact of Covid-19 coronavirus, including with respect to increased remote working</p> <p>The DIFC has issued a Presidential Directive that aims to limit the impact of the Covid-19 coronavirus pandemic on Dubai and includes provisions relating to cybersecurity and data privacy.</p> <p>The directive specifies remote working conditions as an emergency employment measure that organisations can take at this time and specifies related privacy and cybersecurity requirements, such as notifying employees that general monitoring of IT systems and equipment may be ongoing to prevent misuse of employer assets (e.g. information and equipment). If no notification is provided documentation must be produced by the employer to demonstrate clear purpose and benefits of monitoring</p>	<p>The directive is available here (in English and Arabic). The relevant press release is available here.</p>	<p>Cybersecurity and information security Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>technologies in this context to the extent it outweighs the privacy of employees.</p> <p>Employers must ensure adequate cybersecurity measures in place for remote working (to industry standard).</p> <p>Employers are permitted to collect, process and share personal data of employees (including travel, health and Covid-19 coronavirus related symptoms) for any reasonable purpose relating to health and safety of employees or as required by a Competent Authority, though should process no more information than is reasonably necessary.</p> <p>The directive confirms that data subject rights under applicable data protection laws must remain available subject to specific exemptions permissible by law.</p> <p>The directive provides that employers shall maintain a database of employees whose employment has been terminated or who are surplus to need. This information is to be provided to the Government Services Office from time to time, indicating whether employees have given written consent to appear on the DIFC Available Employees Database. The DIFC Available Employees Database may be shared with</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>other Competent Authorities (e.g. UAE Federal Ministry of Health and Prevention, Government of Dubai Health Authority, law enforcement or other federal or local government department authority in the UAE that may impose quarantine restrictions on DIFC employees) maintaining a virtual labour market and will be searchable by employers looking to hire. In such a case, the prospective employer should notify the Government Services Office.</p> <p>The directive also sets out the approach that employers should take to several issues more generally, such as in respect of visas and Covid-19 coronavirus related sick leave.</p>		
<p>United Arab Emirates (Dubai)</p>	<p>Dubai Financial Services Authority (DFSA)</p>	<p>24/3/20</p>	<p>Dubai Financial Services Authority issues statement highlighting increased vulnerability of financial institutions to cyberattacks due to Covid-19 coronavirus</p> <p>The DFSA published a statement confirming that it is closely monitoring the Covid-19 coronavirus pandemic and will take all necessary precautionary and proactive measures to assist Dubai and the wider UAE government in its efforts to contain the spread of the virus.</p>	<p>The statement is available here.</p>	<p>Cybersecurity and information security</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The DFSA's statement sets out the steps it is taking to support the regulated community in the Dubai International Financial Centre (DIFC) and its markets to minimise the financial impact of the pandemic, highlighting that previous investments in regulatory technology and digitalisation have allowed better functionality as many organisations moved to remote working arrangements.</p> <p>The DFSA further encourages financial institutions to be more vigilant to cyber risks due to increased vulnerability of financial institutions to cyberattacks, phishing attempts and fraud. In this light, the DFSA encourages DIFC firms to register to use the DFSA Cyber Threat Intelligence Platform (TIP) and make use of the cyber threat information available on TIP to enhance their cybersecurity at this time, as firms may be more vulnerable to cyberattacks.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
INTERNATIONAL					
International	International Conference of Information Commissioners (ICIC) [Updated as at 21 May 2020]	4/5/20	<p>The ICIC releases a joint statement regarding the importance of continuing to document decisions and transactions during the Covid-19 coronavirus crisis.</p> <p>The ICIC was one of numerous international organisation signatories to a statement calling on both public and private sectors to recognise the importance of effective records management and archives during the crisis.</p> <p>The statement specifically calls for:</p> <ul style="list-style-type: none"> • decisions to be documented; • records and data to be secured and preserved in all sectors; and • security, preservation and access to digital content should be facilitated during lockdown. 	<p>The press release is available here.</p> <p>The statement is available here.</p>	Data protection-general guidance
International	G20 ministers for Digital Economy [Updated as at 21 May 2020]	30/4/20	<p>G20 Ministers for the Digital Economy commit to working together to leverage digital technology in response the Covid-19 coronavirus pandemic.</p> <p>Further to the G20 Leader's Extraordinary Summit of 26 March, the Digital Economy ministers held a virtual</p>	The statement is available here .	Data protection-general guidance Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>meeting at which they committed to amongst other things:</p> <ul style="list-style-type: none"> • work together (with telecoms and ISPs) to maximise inclusive secure and affordable connectivity, keeping networks and infrastructure secure, robust, accessible and resilient and increasing digital capacities (including broadband connectivity, and community networks); • encourage collaboration to collect, pool, process and share, reliable and accurate non-personal information to assist in monitoring Covid-19 coronavirus spread, collecting and processing the same in an ethical, transparent, safe, secure and interoperable manner that protects individuals' privacy and data security. • using computing capacities to accelerate progress in developing, manufacturing, and deploying drug therapies and vaccines, welcoming increased investment in AI research and supporting evidence-based, 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>human-centric, privacy-respecting research and deployment of digital health technologies;</p> <ul style="list-style-type: none"> work together to leverage digital solutions to enable participation in the economy in a manner that respects individual's privacy, security and human rights; and share best practices to enable timely response to counteract malicious cyber activities that present material risk to security of the digital economy and its individuals and business, encouraging online platforms to address disinformation and scams. 		
International	Organisation for Economic Co-operation and Development (OECD)	16/4/20	<p>OECD issues report on privacy and apps in the context of the Covid-19 coronavirus pandemic</p> <p>The OECD's report on privacy and data protection in relation to the use of apps and biometrics notes the increased use of mobile and biometric apps to track and trace the effects of the Covid-19 coronavirus.</p> <p>The report highlights, amongst other things:</p> <ul style="list-style-type: none"> that this use and disclosure of personal information can allow the better identification 	The report is available here.	<p>Mobile apps and new technology</p> <p>Data processing-public authorities</p> <p>Data processing-location data</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>of potential infections, but has implications for data protection;</p> <ul style="list-style-type: none"> • that transparent and accountable privacy solutions should be incorporated by design to balance the advantages of an app with the risks of data collection, processing, sharing and data should only be retained only for so long as necessary for the purpose for which it was collected. <p>The report considers different technology solutions for example:</p> <ul style="list-style-type: none"> • government collaboration with telecommunication service providers to access geolocation data to track population movements (some using mobile call data records) for example: <ul style="list-style-type: none"> ○ Deutsche Telekom providing anonymised "movement flows" data of its users to the Robert-Koch Institute, a research institute and government agency responsible for disease control and prevention. ○ Vodafone Group's Five Point Planto includes providing governments with large 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>anonymised data sets (such as an aggregated and anonymous heat map for the Lombardy region).</p> <ul style="list-style-type: none"> ○ European Commission liaising with eight European telecommunications operators to obtain anonymised aggregate mobile geolocation data, with a view to deleting once the crisis is over. ● New mobile applications for Covid-19 coronavirus "tracking": <ul style="list-style-type: none"> ○ increasingly developed as open source and are the product of partnerships. ○ do not necessarily capture the whole population (e.g. the elderly or those without access to smartphones), nor operate without some error (e.g. distinction between people in the same household and neighbours). ○ examples include Singapore's TraceTogether; European Privacy-Preserving Proximity Tracing; Korea's Tracking App; UK's C-19 COVID Symptom Tracker: potential Apple and Google APIs 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>that enable interoperability between Android and iOS devices using apps from public health authorities.</p> <p>The report highlights some privacy protections and issues arising in the context of geolocation data collection apps. For example, protections include:</p> <ul style="list-style-type: none"> • consent requirements (if not a mandatory app); • not using geo-location data; • local storage of data logs; • encryption; • anonymisation; • indirect exchange of information. <p>For example, concerns include:</p> <ul style="list-style-type: none"> • range of personal data collected; • difficult for users to understand; • apps running in the background; • exchange of information with other apps through APIs generating more detailed information. <p>The report considers using biometric data such as facial recognition including use alongside other technology such as thermal imaging enhanced by AI,</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>to better track citizens. Examples of Russia and Poland are described, in the latter case, where the government launched a biometrics smartphone app to confirm that people remain under quarantine. The report acknowledges privacy concerns particularly when used in the absence of specific guidance or fully informed and explicit consent. Challenges in exercising fundamental rights (e.g. right of access, erasure, amongst others) and inherent bias are also flagged.</p> <p>Examples of privacy by design and default are flagged such as use of data sandboxes for restriction access to data (e.g. Flowminder) and restriction of retention (e.g. Norwegian Institute of Public Health app retains data for 30 days).</p> <p>Key recommendations are:</p> <ul style="list-style-type: none"> • contact-tracing apps should be implemented with full transparency, in consultation with stakeholders, robust privacy-by-design protections, and through open source projects (where appropriate); • governments should consider: <ul style="list-style-type: none"> ○ legal basis of the use 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ proportionality of use of the technologies and data gathering; ○ how the data is stored, processed, shared and with whom (including what security and privacy-by-design protocols are implemented); ○ data quality; ○ whether the public is well-informed with full transparency and accountability; ○ the time period within which more invasive technologies that collect personal data may be used to combat the crisis and for which data can be retained. 		
International	International Criminal Police Organisation (Interpol)	4/4/20	<p>Interpol warns healthcare institutions of ransomware attacks during the Covid-19 coronavirus pandemic</p> <p>Interpol states in its warning "Purple notice" to police in 194 countries of an increased cybersecurity threat. Interpol Cybercrime Threat Response team at Cyber Fusion Centre has detected a significant increase in the number of attempted ransomware attacks against</p>	The press release is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>key organisations and infrastructure engaged in the virus response.</p> <p>The press release highlights that Interpol it is monitoring cyber threats related to the Covid-19 coronavirus, working with those in cybersecurity industry to gather relevant information.</p> <p>The notice:</p> <ul style="list-style-type: none"> • highlights the primary mechanism of attack (ransomware via emails) and the need for mitigation; • encourages hospitals and healthcare companies to, amongst other things: <ul style="list-style-type: none"> ○ regularly update IT systems; ○ backup essential files and store elsewhere; ○ install the latest anti-virus software; ○ use strong passwords. 		
International	Financial Action Task Force (FATF)	1/4/20	<p>FATF issues statement on Covid-19 and measures to combat illicit financing</p> <p>FATF President Xiangmin Liu's statement urges governments to work with financial institutions and</p>	The statement is available here .	Cybersecurity and information security

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>other businesses to utilise the FATF's risk-based approach to address the challenges the Covid-19 coronavirus poses to illicit financing risk. The statement recommends that supervisors, financial intelligence units and law enforcement agencies continue to share information with the private sector, particularly anti-money laundering and countering the financing of terrorism risk (AML/CFT) information.</p> <p>In relation to digital onboarding and simplified due diligence that might be necessary to facilitate confinement or strict social distancing measures in the context of Covid-19, the FATF encourages the use, in line with the FATF Standards, of technology, including Fintech, Regtech and Suptech to the fullest extent possible. The FATF recommends governments to explore how digital identity can be used to aid financial transactions and refers to its recent Guidance on Digital ID. This guidance discusses the benefits of trustworthy digital identity for improving the security, privacy and convenience of identifying people remotely, which can be used for onboarding and conducting transactions, while also mitigating money laundering and terrorism financing risks.</p>		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
International	Council of Europe [Updated as at 21 May 2020]	28/4/20	<p>Council of Europe issues a joint statement on digital contact tracing</p> <p>The Council of Europe's Chair and Data Protection Commissioner issued a joint statement on digital contract tracing.</p> <p>The statement first asks whether mobile contact tracing apps are indeed the solution and whether risks associated with them are worth taking if efficacy has yet to be shown. In any event, it considers that given the potential impact of mobile apps on privacy and data protection, it is crucial to ensure that measures relating to data processing are necessary and proportionate in relation to a legitimate purpose purpose and that they reflect, at all stages, a fair balance between all interest concerned the rights and freedoms at stake and the ECHR and Convention 108+ requirements.</p> <p>Considering issues in more detail the statement:</p> <ul style="list-style-type: none"> • highlights that despite the voluntary nature of the apps in general, consent will not necessarily be the legal basis for processing personal data and recourse to processing on 	<p>The press release if available here.</p> <p>The statement is available here.</p>	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>the basis of public interest may be effective subject to safeguards;</p> <ul style="list-style-type: none"> • suggests that design of apps should be completed in such a manner as to minimise risk of interference with fundamental rights and freedoms and to ensure, for example, that location data is not used, no direct identification is possible and re-identification is prevented. Data used for contact tracing should also be kept for the duration of the pandemic only with limits set based on relevance of data, deletion to follow and automatic deactivity of the application incorporated; • considers that further processing of data for research of statistical purposes beyond the original tracing purpose would require explicit consent; • highlights additional conditions applicable to processing of health related data, the need to avoid use of location data, to ensure quality and accuracy of data and restrict processing of data to a minimum; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> • emphasises that provisions addressing automated decision making continue to apply; • considers that app users should not be directly identified, that any identifiers should be cryptographically strong and frequently renewed, that systems should invoke strong encryption and security more generally and that decentralised structures are preferred; • expects interoperability of apps; • recommends full transparency of development (including open source code) and use and oversight and independent audit. 		
International	Council of Europe	30/3/20	<p>Council of Europe issues statement on data protection and Covid-19 coronavirus</p> <p>The Council of Europe's Chair and Data Protection Commissioner issued a joint statement on data protection and the Covid-19 coronavirus.</p> <p>The statement:</p> <ul style="list-style-type: none"> • makes it clear that personal data must be protected even in the context of the crisis where measures taken to fight the pandemic 	<p>The press release is available here.</p> <p>The statement is available here.</p>	<p>Data protection-general guidance</p> <p>Data processing-employment</p>

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>and maintain business and education activities can put them at risk;</p> <ul style="list-style-type: none"> • clarifies that data protection should not be a barrier to life saving especially given data protection principles allow a balancing assessment to be made; • highlights that the high standards of data protection expected by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) and Convention 108+ are compatible with other fundamental rights and relevant public interests; • provides examples of protections that should be respected: <ul style="list-style-type: none"> ○ data subjects informed of processing; ○ processing only if necessary and proportionate to the explicit, specified and legitimate purpose pursued; ○ impact assessment before the start of processing; 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<ul style="list-style-type: none"> ○ privacy by design is ensured; ○ appropriate measures adopted to protect the security of data especially when special category data; ● flags that restrictions imposed should be provisional with safeguards in place and concrete measures and procedures regarding the return to "normal" data processing regimes; ● notes that anonymised data (e.g. that used in epidemiologic monitoring) is not covered by data protection requirements and therefore aggregate location data (e.g. as used to determine gatherings) is not prevented by data protection requirements; ● provides advice on employer processing of data, processing of health data, large scale data processing, mobile data processing and educational processing; and ● reminds readers that the Council of Europe has developed a series of relevant recommendations and guidelines. 		

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
International	Global Privacy Assembly (GPA) [Updated as at 28 May 2020]	27/5/20	<p>GPA announces Covid-19 coronavirus taskforce</p> <p>The GPA has announced the creation of a Covid-19 coronavirus taskforce, designed to drive practical responses to privacy issues emerging from the Covid-19 coronavirus pandemic.</p> <p>Its remit is also to assist GPA members with insight and best practices and will look to the membership for expertise.</p> <p>The taskforce met on 26 May and discussed the most strategic and key privacy issues to examine initially, agreeing a workplan with a view to communicating progress to the GPA membership and wider audience.</p>	The press release is available here .	Data protection-regulator approach
International	Global Privacy Assembly (GPA)	21/5/20	<p>GPA issues a statement on Privacy by Design in contact tracing in the context of the Covid-19 coronavirus</p> <p>The GPA's statement noted that the success of contact tracing apps will depend on the trust of individuals, and that wider ethical considerations have been addressed, as contact tracing apps are developed for the wider good.</p>	The statement is available here .	Mobile apps and new technology

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>The GPA considers privacy by design to be a key enabler of innovation with DPIAs focusing attention as required. It sets out questions to consider when engaging in contact tracing but notes that points raised in the statement apply equally to other developments in the fight against Covid-19 coronavirus, such as temperature checking and immunity passports.</p>		
International	Global Privacy Assembly (GPA)	17/3/20	<p>Global Privacy Assembly's Executive Committee issues statement on the Covid-19 coronavirus and data protection</p> <p>The Executive Committee of the Global Privacy Assembly (GPA, the former International Conference of Data Protection and Privacy Commissioners) issued a statement on the Covid-19 coronavirus and data protection.</p> <p>The GPA anticipates that the data protection principles in law will enable the use of data in the public interest whilst offering expected protections.</p> <p>Amongst other things, the statement highlights that whilst health information is considered sensitive in many jurisdictions, the GPA is supportive of public bodies and health practitioners communicating</p>	<p>The statement is available here.</p> <p>The resources page is available here.</p>	Data protection-general guidance

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source	Topic area
			<p>directly with people, and scientific and government bodies, to coordinate nationally and globally to tackle the Covid-19 coronavirus.</p> <p>The GPA has also created a resources page on data protection and the Covid-19 coronavirus.</p>		

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

© Allen & Overy LLP 2020. This document is for general guidance only and does not constitute definitive advice. | UKC1: 2000071163.12