ALLEN & OVERY

Covid-19 update

CYBERSECURITY AND INFORMATION SECURITY DEVELOPMENTS

19 June 2020

We set out below a high-level summary of recent guidance issued by regulators across the world, addressing the changing cybersecurity risk profile and cybersecurity and information security requirements for companies and other organisations arising as a consequence of the Covid-19 coronavirus pandemic.

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). Earlier this month we had updated Canada, India, Japan, Czech Republic, France, Germany, Poland, UK (CDEI) and the EDPB, reflecting the latest publications as at 4 June 2020. This week we have added Philippines and further updated the UK, reflecting the latest publications as at 18 June 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.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
AMERICAS				
Canada [Updated as at 4 June 2020]	Canadian Centre for Cyber Security (**CCCS**)	27/5/2020	**CCCS publishes a cyber threat bulletin on the impact of Covid-19 coronavirus on cyber threat activity** Targeted at the cybersecurity community, the bulletin sets out a number of key judgements, assessing the risk of cyber threats as increasing due to the Covid-19 coronavirus pandemic. Amongst other things, it considers that almost certainly ransomware will continue to target healthcare and medical research facilities, Canadian IP and classified information will be a target and the remote workforce will be increasingly targeted by foreign intelligence services and cybercriminals. The bulletin goes on to discuss how malicious actors have already taken advantage of the pandemic, using it as a thematic lure or subterfuge for their activities, such as cyberespionage and cybercrime. It calls out phishing attacks (impersonating public health and other international organisations for example), use of malware and ransomware, and exploitation of remote access protocols, video conferencing as particular issues.	The bulletin is available here.
Canada	Canadian Centre for Cyber Security (**CCCS**)	15/3/20	**Canadian Centre for Cyber Security issues guidance on Cyber Hygiene in relation to the Covid-19 coronavirus** 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	The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			official health agencies. The guidance reminds individuals to be wary of malicious emails and attachments.	
Mexico	Mexican National Institute of Access to Information and Data Protection (**INAI**)	8/4/20	**INAI publishes recommendations on remote working related to Covid-19 coronavirus pandemic** 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. The INAI recommendations include, amongst others: • 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;	The guidance is available here (only in Spanish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• using secure access control measures, such as strong passwords, multi-factor authentication and encryption to restrict access to the device and reduce risk of compromising the security of personal data; • 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	**INAI releases statement requesting extreme caution on use of personal data of Covid-19 coronavirus patients** 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. 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 recommendations for personal data processing in this context, including: • 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;	The statement is available here (only in Spanish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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 disclosed. If personal data disclosure to health authorities is required, this must be clearly documented, substantiated and carried out with due appropriate security measures; • 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
USA	The Cybersecurity and Infrastructure Security Agency (**CISA**) The U.S. Department of Homeland Security (**DHS**) The UK National Cyber Security Centre (**UK NCSC**)	5/5/20	**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** 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). 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. 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.	The NCSC news report and alert are available here and here. The CISA press release is available here. The CISA alert is available here. The joint advisory is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The joint advisory report goes on to descibe a number of mitigations including: • 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. 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.	
USA	Cybersecurity and Infrastructure Security Agency (**CISA**)	8/4/20	**CISA issues teleworking guidance on securing networks and cloud environments used by the federal workforce** 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	The press release is available here. The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			use collaboration tools. Connections to the public internet will continue to route through the National Cybersecurity Protection System EINSTEIN. Guidance: • 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 information will need to be provided to CISA for cybersecurity analytical purposes; • informs agencies that the interim guidance provided under Agency Teleworker Option 3 provides additional temporary relief with additional security patterns. 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. The guidance is short term and will be phased out, though features will be integrated in longer term guidance.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			Though the guidance is applicable to federal agencies, the risks and issues covered can be more generally applicable to private organisations.	
USA	The Department of Health & Human Services (HSS) Office for Civil Rights (**OCR**)	20/3/20	**OCR issues further guidance on telehealth remote communications following its Covid-19 coronavirus Notification of Enforcement Discretion** 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). Amongst other things, the FAQs clarify that: • 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 coronavirus emergency, the enforcement discretion does not apply to health insurance companies that pay for telehealth services; • 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 press release is available here. The FAQs are available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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 the patient move to a reasonable distance from others during the discussion); • 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
USA	National Institute of Standards and Technology (**NIST**)	19/3/20	**NIST releases a bulletin regarding telework security** NIST published an Information Technology Laboratory Bulletin on Telework Security (the **Bulletin**) as millions of Americans transitioned to their homes to continue to work. 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 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. The Bulletin includes information regarding: • 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.	The press release is available here. The Bulletin is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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: • two Cybersecurity Insights blog posts on *1)* Telework Security Basics *and 2)* Preventing Eavesdropping and Protecting Privacy on Virtual Meetings; and • 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	**OCR intends to use discretion in enforcing HIPAA violations related to video chat services in context of the Covid-19 coronavirus pandemic** 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. 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	The press release is available here. The notification is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			chat, Google Hangouts video, or Skype, where they are used in good faith for remote healthcare or diagnostic purposes. Importantly, the services provided using these methods need not be directly related to the Covid-19 coronavirus. This exercise of discretion does not apply to use of public facing apps such as Facebook Live, Twitch, TikTok, or similar.	
USA	The US Department of Homeland Security (**DHS**) The Cybersecurity and Infrastructure Security Agency (**US CISA**) The UK National Cyber Security Centre (**UK NCSC**)	8/4/20	**UK NCSC and the US CISA publish a joint advisory on malicious cyber activity exploiting the Covid-19 coronavirus pandemic** 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. The advisory notes that APT groups and cybercriminals are actively using the pandemic for commercial gain, deploying various threats, including: • 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	The press statement of the US CISA is available here. The press statement of the UK NCSC is available here. The advisory is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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. Recommendations for organisations include: • 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; • ensuring teleworking policies address physical and information security requirements; • planning for successful phishing attacks; and • educating employees in identifying and reporting suspected phishing emails. The advisory also identifies key online resources published by the UK NCSC and US CISA in relation to mitigating risk online, including: • 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;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- NCSC guidance to help spot, understand and deal with suspicious messages and emails, guidance on phishing for organisations and cybersecurity professionals, and other materials.	
USA	Cybersecurity and Infrastructure Security Agency (**CISA**)	13/3/20	**CISA issues guidance on VPN security and working from home in the context of Covid-19 coronavirus** The CISA published an alert on VPN security and working from home. In particular, the alert highlights the need to: - 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.
USA	Financial Industry Regulatory Authority (**FINRA**)	9/3/20	**FINRA releases a regulatory notice on Covid-19 coronavirus business continuity planning, guidance and regulatory relief** The FINRA released a regulatory notice on Pandemic-Related Business Continuity Planning, Guidance, and Regulatory Relief. Amongst other things, as part of pandemic preparedness, the notice highlights that firms should consider the increased threat of cyber events (e.g. systems being	The notice is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			compromised through phishing attacks), due to the use of remote offices or telework arrangements. 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.	
APAC				
Australia [Updated as at 28 May 2020]	Australian Cyber Security Centre (**ACSC**)	22/5/20	**ACSC publishes guidance for critical infrastructure providers concerning cybersecurity during the Covid-19 coronavirus pandemic** The ACSC has published cybersecurity guidance directed at critical infrastructure providers (e.g. power and water providers), particularly addressing remote working practices.	The press release is available here. The guidance is available here.
Australia	Australian Cyber Security Centre (**ACSC**)	8/5/20	**ACSC warns of APT actors targeting health sector organisations and Covid-19 coronavirus essential services** 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. 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, Australian	The warning is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			health sector entities have been impacted by Coronavirus-related phishing attacks. The ACSC recommended certain cybersecurity mitigations including, amongst other things: • multi-factor authentication; • blocking macros; • regular updates; • patching of software; and • email content scanning. The ACSC reminded readers of its ReportCyber web portal for reporting cyber incidents.	
Australia	Office of the Australian Information Commissioner (**OAIC**)	1/4/20	**OAIC issues a statement on Covid-19 and protection of personal information** 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: • "need-to-know" basis for using and disclosing personal information of individuals (including health information);	The statement is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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 potential or confirmed Covid-19 case in the workplace; - implementing appropriate security measures, including where employees are working remotely.	
Australia	Office of the Australian Information Commissioner (**OAIC**)	18/3/20	**OAIC issues guidance on using and disclosing personal information including regarding remote working** 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: - 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 but should only use or disclose personal information that is reasonably necessary in order to prevent or manage	Coronavirus (COVID-19): Understanding your privacy obligations to your staff is available here. Guidance on the employee records exemption is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			Covid-19 in the workplace. Whether disclosure is necessary should be informed by advice from the Department of Health. • 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 prevent a serious threat to the life, health or safety of an individual, or to public health or safety. 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. Amongst other measures they should: • increase and test cybersecurity measures;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• ensure devices have up-to-date security and are stored safely when not in use; • use work – not personal – email accounts; • implement multi-factor authentication for remote access. 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.	
Australia	Australian Cyber-security Centre (**ACSC**)	13/3/20	**ACSC issues guidance on good cybersecurity measures to address the cyber threat in preparing for the Covid-19 coronavirus** The ACSC recommends incorporating proactive strategies, including: • 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.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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.	
Hong Kong (SAR), China	Office of the Privacy Commissioner for Personal Data (**PCPD**)	30/3/20	**PCPD issues guidance for employers and employees in relation to Covid-19 coronavirus** The PCPD issued brief guidance addressing the data privacy issues related to the Covid-19 coronavirus pandemic in the employment context. 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. 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 particular situation. Collecting additional data must still adhere to the principles of data	The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			minimisation, purpose specification and use limitation. It must be necessary, appropriate and proportionate to the intended purpose. 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.	
India [Updated as at 4 June 2020]	Data Security Council of India (**DSCI**)	24/5/2020	**DSCI publishes a paper on Business Resiliency and Security during the Covid-19 coronavirus pandemic.** Security leaders from different industries and DSCI shared experiences, learning, and best practices in relation to the Covid-19 coronavirus pandemic in a series of calls. The paper compiles the discussion (including guidance issued on 5 May 2020) and is an account of how the security community handled the challenges of the pandemic. In particular, the paper discusses remote working options (e.g. VPN) and best practices and challenges. It also references the Department of Transport’s guidance on remote working for “Other Service Providers” of 13 and 15th April and the extension of a relaxation of permissions requirement until end July 2020. The paper considers business resilience and continuity planning for a range of Covid-19 coronavirus scenarios (including a recurrence of the Covid-19	The paper is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			coronavirus). It also notes suggestions for managing cybersecurity, including amongst other things, noting the need for a cyber maturity assessment and highlighting network security actions (e.g. patching, configuration, health check ups). The paper flags proposals of CISOs that organisations should secure data by encrypting and monitoring connection channels and traffic, securing protocols to access data, classifying data, looking at data leak prevention, considering user behaviour monitoring, forensic investigation, information rights management. DSCI provides best practice tips for use of video conferencing and collaboration tools and considers that they should be assessed before use against four criteria: security controls (in-built), privacy (compliance with GDPR for example), compliance with international standards (e.g. ISO27001), and integration (with other systems and apps). Finally, the paper notes the need for legal compliance and amongst other things, calls out the need for data protection and cybersecurity law compliance	
India	Data Security Council of India (**DSCI**)	5/5/2020	**DSCI publishes guidance on returning to work as restrictions begin to lift in relation to the Covid-19 coronavirus pandemic** The DSCI has consolidated output from discussions with CISOs over the previous 7 weeks, and considered “How should organizations roll-out their strategy for return to work from office under new circumstances?”	The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The guidance covers three key areas: people, processes and technologies. Amongst other things the guidance details a 6 phase approach to technological and administrative controls. This addresses: user awareness of best practices for moving from home to office working; workforce planning and availability of critical resources; infrastructure readiness; deployment of "hardening" standards, and baseline security; scanning and sanitization of machines to avoid vulnerabilities; planning and allowing access to different network zones; monitoring network behaviour and re-configuring rules based on use-cases; sharing of information between IT and business. In relation to treatment of technologies, IT and cybersecurity teams must re-evaluate the security baselines and ensure adherence across devices. Ongoing patching of vulnerabilities is essential and management of BYOD needs policy intervention. Technology to enable remote working should remain available.	
India	Data Security Council of India (**DSCI**)	24/4/20	**DSCI publishes a DSCI Privacy Outlook Advisory, considering data protection during the Covid-19 coronavirus pandemic** The Privacy Outlook, in the form of a DSCI Advisory (the **Advisory**) highlights the privacy implications of the Covid-19 coronavirus for various stakeholders and advises on privacy and data protection practices. The Advisory addresses healthcare privacy conditions, noting the importance of: • notifying patients of all information and personal data collected;	The Advisory is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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. The Advisory notes that, whilst collecting data to help contain and track the Covid-19 coronavirus, government authorities must be mindful of data protection principles, in particular collection and use limitation to ensure collection of personal data is necessary and proporationate. The Advisory goes on to specify that: • 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;	

Jurisdictions/ locations **(by region and alphabet)**	**Supervisory authority or regulator**	**Date**	**Summary**	**Source**
			• 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; • 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. 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.	
India	Data Security Council of India (**DSCI**)	22/4/20	**DSCI publishes guidance for cybersecurity in specific industries in light of Covid-19 coronavirus pandemic and cyberattack warning** 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 Cyberattack Advisory is available here and the technical report is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			the cyberattacks vary in nature but that the Maze ransomware attack is particularly prevalent. 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. The DSCI's publications on Maze ransomware follow its issuance of four DCSI Advisories for specific industries and groups including in response to increased cybersecurity risk due to the Covid-19 coronavirus pandemic. Specifically, the DSCI has issued the following guidance in its Advisories: • 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	The portal for the DSCI Advisories is available here. The Advisories themselves are available here (employees), here (healthcare industry) and here (law enforcement).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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 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 • 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	Data Security Council of India (**DSCI**)	18/3/20	**DSCI publishes recommendations on security measures for working from home** The DSCI has published an recommendations in an Advisory document on working from home. The advisory document outlines requirements to secure companies' networks whilst allowing remote access for employees.	The press release is available here. The Advisory document is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. The document also advises companies to provide live 24/7 IT support and ensure staff follow basic security practices and procedures, which include: • strong password policies; • firewalls; • awareness of increased phishing attack threats; and protection of confidential information when working from home.	
Japan [Reviewed as at 4 June 2020]	National Centre of Incident Readiness and Strategy for Cybersecurity (**NISC**)	14/4/20	**NISC publishes guidelines on teleworking security in light of Covid-19 coronavirus pandemic** 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. The document provides guidance on the precautions to be taken for teleworking in a government agency context and for important infrastructure	The guidelines are available here (only in Japanese).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			operators. The NISC emphasises that it is important for such agencies to understand the security risks of teleworking and manage these appropriately. 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 standards that government agencies are expected to meet. 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.	
New Zealand [Updated as at 28 May 2020]	National Computer Emergency Response Team (**CERTNZ**)	25/5/20	**CERTNZ releases cybersecurity guidance on measures for working from home** CERTNZ has published guidance on cybersecurity issues when working from home including, amongst other things: • use remote access software; • create strong passwords;	The guidance is available here. The associated quick reference guide is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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 • record all remote working decisions/requirements in a policy. An associated quick guide has also been produced for ease.	
Philippines [Updated as at 18 June 2020]	Department of Information and Communications Technology (**DICT**)	17/6/20	**DICT publishes a blog supporting Securities Exchange Commission (SEC) in its call for greater cybersecurity and data protection efforts in light of the Covid-19 coronavirus pandemic** The DICT blog relates to a recent notice issued by SEC which encouraged corporations to assess their exposure to cybersecurity risks and develop appropriate policies and measures to address the same. Following the SEC notice, DICT offers its Philippine National Public Key Infrastructure (**PNPKI**) services, to the private sector. These services include issuance of digital certificates to ensure confidentiality, authenticity, integrity and non-repudiation of electronic transactions and documents.	The blog is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The DICT also conducts vulnerability assessment and penetration testing services for its clients through its Cybersecurity Bureau and advises corporations to report cybersecurity incidents in their systems to the DICT's Cybersecurity Bureau. This is particularly relevant as there is a transition to the "new normal" and a greater reliance on ICT**.**	
EUROPE				
EU	**European Parliament [Reviewed as at 21 May 2020]**	1/4/20	**The European Parliament has published recommendations on how to protect yourself from cybercrime in the context of the Covid-19 coronavirus** The European Parliament notes that increased time online and homeworking can lead to unsafe online practices and opportunities for cybercriminals to exploit weaknesses. 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: • 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;	The recommendations are available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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; • fake messages about non-existent package deliveries. 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: • 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
EU	European Commission [Reviewed as at 21 May 2020]	16/4/20	**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** 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). 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: • essential apps requirements, including the epidemiological framework, technical functionalities, cross-border interoperability requirements and cybersecurity measures and safeguards;	The press release about the Toolbox is available here. The Toolbox is available here. The press release about the data protection guidance is available here. The Data Protection Guidance is available here. The Recommendation is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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. **Apps with decentralised processing versus backend server solution** 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: - 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	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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 Public health authorities would not have access to any anonymised and aggregated information on 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; • 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 guidance. In such a case, the user should express his/her consent. 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	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. **Cybersecurity** 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. 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. **Next steps** 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	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			duration of the pandemic. The European Commission will publish by 30 June 2020 a progress report and proposals for further follow-up actions. 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. 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.	
EU	**European Commission, European Parliament, Council of the European Union**	23/4/20	**Date of application of the EU Medical Devices Regulation postponed due to the Covid-19 coronavirus pandemic** 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. The decision is intended to prevent unnecessary shortages and delays in medical equipment supplies during the Covid-19 coronavirus pandemic,	The notification about postponed application is available here. The Regulation amending MDR is available here. The press release of the European

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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 MDR was published in the Official Journal of the EU on 23 April 2020 and came into force immediately.	Parliament is available here. The press release of the European Commission is available here.
EU	**European Banking Authority (EBA)**	22/4/20	**EBA publishes statement on additional supervisory measures relevant during the Covid-19 coronavirus outbreak** The EBA has published a statement on supervisory measures it will employ in the context of the Covid-19 coronavirus crisis. 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. With regards to operational resilience, the statement highlights its importance in order to ensure business continuity, adequate information and communication 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	The press release is available here. The statement is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. Given that financial institutions are required to make every effort to comply with EBA Guidelines: the EBA calls on financial institutions to: • 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 involvement of management in effective decision-making and priority setting; • 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;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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; • 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. The EBA: • 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 ongoing basis and to limit losses in the event of severe business disruption).	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
EU	European Insurance and Occupational Pensions Authority (EIOPA)	17/4/20	**EIOPA issues statement on mitigating the impact of Covid-19 coronavirus pandemic on the occupational pensions sector** 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. 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.	The press release is available here. The statement is available here.
EU	EUROPOL	3/4/20	**EUROPOL issues a report addressing cybersecurity risk in the context of the Covid-19 coronavirus** 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. This includes analysis regarding: • ransomware; • DDoS;	The report is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• child sexual exploitation; • the dark web; • hybrid threats: disinformation and interference campaigns.	
EU	European Commission **Computer Emergency Response Team for the EU Institutions (CERTEU)** European Union Agency for Cybersecurity (**ENISA**) European Union Agency for Law Enforcement Cooperation (**Europol**)	20/3/20	**The European Commission, ENISA, Europol, and CERT-EU issue a statement on the Covid-19 coronavirus outbreak** The European Commission, ENISA, Europol, and CERTEU issued a joint statement to highlight that they are coordinating efforts to track potential malicious cyber activities in the context of an increased number of people working from home during the Covid-19 coronavirus outbreak.	The European Commission's press release is available here. ENISA's press release is available here. Europol's press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
EU	EU Agency for Cybersecurity (ENISA) [Updated as at 21 May 2020]	18/5/20	**ENISA issues recommendations on security of smart infrastructure during the Covid-19 Coronavirus crisis** 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. It suggests, with regards to home premises (where many currently work): • 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. With regards to business premises, amongst other things: • 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	The press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• preparing and updating incident response plans according to the current risks.	
EU	EU Agency for Cybersecurity (**ENISA**)	11/5/20	**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** ENISA highlights the redirection of resources to the primary healthcare goal as creating vulnerability in the healthcare sector with risk exacerbated by: • 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. As such, ENISA recommends: • sharing vulnerability information with healthcare staff, building awareness of the situation (including through campaigns) and, in the case of cyber infection, asking staff to disconnect from the network to contain the spread;	The advice is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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	**ENISA publishes recommendations regarding phishing during the Covid-19 coronavirus outbreak** 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): • reflect on a request for your personal information and whether appropriate; • 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;	The press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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. ENISA recommends that victims of a phishing attack should: • 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
EU	EU Agency for Cybersecurity (**ENISA**)	4/5/20	**ENISA publishes guidance on Computer Security Incident Response Teams (CSIRT) and their relevance during the Covid-19 coronavirus crisis** 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. 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. The guidance also draws attention to training and materials available should an organisation want to set up an incident response team.	The guidance is available here. The map is available here.
EU	EU Agency for Cybersecurity (**ENISA**)	27/4/20	**ENISA publishes advice to SMEs when choosing online communication tools in the context of the Covid-19 coronavirus outbreak** 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: • make sure that the tool supports encrypted communication;	The advice is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• choose a tool that supports centralised management (such as call restriction and password policy); • 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	**ENISA publishes recommendations for teleworking and warns against phishing scams related to Covid-19** ENISA published a brief guidance with recommendations on maintaining adequate level of cybersecurity for employers and employees on remote working in the context of Covid-19 coronavirus.	The press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The recommendations for employers mirror the guidance issued on 15 March 2020 and include, amongst other things: • 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-date security software and security patch levels; • 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;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• processing of employee data in the context of teleworking (e.g. time keeping) should be compliant with data protection law. Employees are recommended to, amongst others, when teleworking: • 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 systems and avoid the exchange of sensitive corporate information through possibly insecure connections; • 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. ENISA also issued a warning against growing number of phishing attacks exploiting the Covid-19 coronavirus pandemic. ENISA recommends utmost	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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 verified before any links are clicked or attachments are opened.	
EU	EU Agency for Cybersecurity (**ENISA**)	15/3/20	**ENISA issues a brief note on remote working** ENISA published a brief note with recommendations for employers on remote working in the context of Covid-19 coronavirus. Amongst other things, it is recommended that employers: • 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. The note also highlights the increased risk of phishing attacks and what to look out for.	The note is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Austria	Austrian supervisory authority (**DSB**)	27/3/20	**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** The DSB updated its page dedicated to guidance on Covid-19 coronavirus and processing of personal data and related documents. In particular, the DSB clarified the following: • 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 in the field of public health) and in accordance with Section 5 (3) of the Epidemic Act 1950; • 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;	The guidance is available here. The FAQs are available here. The security of remote work guidance is available here. The model form is available here. (all only in German)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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. 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.	
Denmark	Danish Datatilsynet	16/3/20	**Danish Datatilsynet publishes data protection recommendations for home working** 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: • 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;	The recommendations are available here (only in Danish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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 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. The Danish Datatilsynet further referred to the guidance issued by the Center for Cyber Security on 15 March 2020.	
Denmark	Centre for Cybersecurity (**CCS**)	24/4/20	**CCS publishes recommendations on cybersecurity practices for return to work** 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. In particular, the Recommendations provide high level guidance to employees including: - ask IT support about how the IT equipment that has been with you at home or is shared can be cleaned;	The press release is available here. The Recommendations are available here. (both only in Danish)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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 private information on the including usernames and passwords stored in the browsers; - 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. With respect to employers, the Recommendations: - 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;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• suggest rectifying operating conditions that have not been managed fully during the crisis e.g. scheduled service maintenance; • 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	**CCS issues a statement on system vulnerabilities caused by increased use of remote access stemming from Covid-19 coronavirus** The CCS highlighted in its statement several instances in which VPN gateway vulnerabilities have been exploited to compromise networks with, amongst other things, ransomware. 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. Finally, the CCS outlined that another tool for remote access is remote desktop protocol which, amongst other things, should be protected by two-factor authentication.	The press release is available here (only in Danish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Denmark	Center for Cyber Security (**CCS**)	1/4/20	**Center for Cyber Security issued five cybersecurity advisories for individuals to address malicious actions related to Covid-19 coronavirus** 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.	The press release is available here (only in Danish). The page with five advisories is available here (only in Danish).
Denmark	Center for Cyber Security (**CCS**)	31/3/20	**Center for Cyber Security publishes guidance on security of communication and collaboration platforms used for homeworking during Covid-19 coronavirus pandemic** 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: • 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;	The press release is available here and the guidance here (both only in Danish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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.	
Denmark	Center for Cyber Security (**CCS**)	27/3/20	**Center for Cyber Security publishes guidance on protecting RDP access** 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. The guidance encourages IT security officers to: • 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	The guidance is available here (only in Danish). The CCS password guide is available here (only in Danish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- close all redundant employee accounts.	
Denmark	Center for Cyber Security (**CCS**)	15/3/20	**CCS issues a threat assessment for the use of home workplaces in light of Covid-19 coronavirus** 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. 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. The threat assessment lists recent examples of malware attacks using fake Covid-19 Coronavirus websites and phishing emails claiming to represent health authorities. The CSS further issued a list with practical tips for organisations and employees to ensure security of remote working from home.	The press release is available here. The threat assessment is available here. The list with tips is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
France [Reviewed as at 18 June 2020]	National Cybersecurity Agency of France (**ANSSI**)	27/4/20	**ANSSI announces project team developing StopCovid app pilot and clarifies its role in ensuring cybersecurity aspects of the app** The French government launched a pilot project for the development of an app and related infrastructure (**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. The StopCovid project aims at development of a contact tracing mobile app based on the following principles: • 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; • transparency, which includes publication of the developed app under open source license and ensuring transparency of algorithms, open	The press release announcing the StopCovid project team is available here (only in French). The press release describing the role of ANSSI is available here (only in French).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. At European level, the project will be carried out in close collaboration with national teams developing comparable applications in Germany, the UK, Italy, Spain and Norway, with expectation to develop interoperable solutions. The ANSSI also published its recommendations to INRIA on the information security aspects of the StopCovid pilot. The recommendations include, amongst others: • 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;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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.	
France	French supervisory authority (**CNIL**)	9/4/20	**CNIL publishes guidance on videoconference tools in the context of Covid-19 coronavirus** 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: • 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; • verify that the app provider has implemented essential security measures (such as end-to-end encryption of communications);	The guidance is available here (only in French).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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**)	1/4/20	**CNIL publishes recommendations regarding teleworking and security measures in the context of the Covid-19 coronavirus** The CNIL recommends that organisations implement additional measures to secure information systems for teleworking. In particular, the CNIL recommends: • 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; • equipping all workstations of employees, at a minimum, with a firewall, antivirus and tooling to block access to malicious websites;	The recommendations for organisations are available here. The recommendations for employees are available here. (only in French).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• setting up a VPN as soon as possible and enabling two-factor VPN authentication. For organisations providing online services, the CNIL recommends: • 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; • 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. The CNIL also published recommendations regarding teleworking on 1 April 2020 directed at employees, reflecting the recommendations outlined for organisations.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
France	Cybermalveillance	16/3/20	**Cybermalveillance publishes guidance on cybersecurity pitfalls and best practices in context of Covid-19 coronavirus** The Cybermalveillance published guidance on best cybersecurity practices and pitfalls to avoid in the context of the Covid-19 coronavirus pandemic. 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. 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 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. Organisations are called upon to implement additional security measures to prevent cyberattacks including: • applying, without delay, security updates to devices connected to corporate networks; • enabling two-factor authentication procedures for teleworking; • enforcing strong password policies;	The guidance is available here (in French only).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- creating regular backups for data, including a backup not connected to the primary facility.	
Germany [Updated as at 4 June 2020]	German Parliament (**Bundestag**)	22/4/20	**Bundestag adopts resolution and report on tele- and video-conferencing for works councils** The Bundestag approved a resolution and report from the Bundestag Committee on Labor and Social Affairs in relation to the draft law, "*Arbeit-von-morgen-Gesetz*" ("Work of Tomorrow Act" – *Gesetz zur Förderung der beruflichen Weiterbildung im Strukturwandel und zur Weiterentwicklung der Ausbildungsförderung*). The resolution and report proposed amendments to the draft law, including to: - allow certain works councils, employee representative bodies, and youth and trainee representative bodies to attend meetings and adopt resolutions via video and telephone conferencing (applied retroactively from 1 March 2020); - 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.	The resolution and report are available here (in German only). The draft law is available here (in German only)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Germany	Federal Commissioner for Data Protection and Freedom of Information (**BFDI**)	27/3/20	**BFDI publishes a compilation of guidance on data protection in relation to Covid-19 Coronavirus** 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. 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. The overview currently covers processing personal data in employment relationship, sharing mobile and geolocation data with government, processing data of visitors, general guidance on processing personal data and health data, and on working from home.	The note is available here (in German only).
Germany	Schleswig-Holstein DPA	4/5/20	**Schleswig-Holstein DPA issued a statement warning against Covid-19 coronavirus spam** The Schleswig-Holstein DPA issued a statement warning against Covid-19 coronavirus spam. The Schleswig-Holstein DPA recommends internet users to carefully verify emails supposedly sent by authorities and banks. Spammers are currently falsely using email addresses that look similar to	The press release of the Schleswig-Holstein DPA is available here (German only).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			valid email addresses of such institutions with schemes such as *corona-zuschuss@<name of the bank>.de.com* (for example *corona-zuschuss@ib-sh.de.com*). Recipients of those emails are asked to provide certain data (often via PDF documents) for control purposes, which – instead of banks or authorities – spammers gain access to.	
Germany	Schleswig-Holstein DPA	24/3/20	**Schleswig-Holstein DPA publishes guidance on data protection issues of home working related to Covid-19 coronavirus** 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. Certain confidential work should not be carried out at home. 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.	The press release is available read here (only in German). The Guidance is available here (only in German).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The Schleswig-Holstein DPA recommends that organisations should implement written policies for employees for remote working if they have not done so already.	
Germany	Rhineland Palatinate DPA	8/4/20	**Rhineland-Palatinate DPA issues statement on IT security in hospitals** The Rhineland-Palatinate DPA issued a statement on IT security in hospitals during the Covid-19 coronavirus pandemic. The DPA emphasises the importance of appropriate IT security during a crisis and outlined that in particular health sector structures and hospitals are highly exposed and can be victims of cyberattacks. It also expresses its concerns regarding digital solutions that are currently implemented in a provisional manner due to the Covid-19 coronavirus but do not meet the required standards of IT security. Even though the DPA acknowledges the reasons for such measures being implemented during a pandemic in such a manner, it nevertheless considers it this a risk if those measures remain unaltered after the crisis and are not re-evaluated in the future. The DPA also refers to the recommendations of the “Roundtable IT Security in Hospitals” in its statement, which contains guidance for hospitals to support them in preventing and addressing cyberattacks.	The statement on IT security of the DPA is available here . The recommendations of the “Roundtable IT Security in Hospitals” here. (both in German only).
Germany	Berlin DPA	2/4/20	**Berlin DPA created a dedicated information site on Covid-19 coronavirus guidance discussing home working** The Berlin DPA has provided a section of its website with guidance related to data protection issues in the context of Covid-19 coronavirus.	The website is available here (only in German). The guidance on home working is

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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.	available here (only in German).
Germany	Baden-Wuerttemberg DPA	27/3/20	**Baden-Wuerttemberg DPA published guidance on data protection-friendly communication tools in light of the Covid-19 coronavirus** The Baden-Wuerttemberg DPA published guidance for organisations on data protection-friendly communication tools, with an emphasis on videoconferencing systems. 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. 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. The Baden-Wuerttemberg DPA further recommends considering whether a videoconferencing solution will entail processing personal data outside the	The guidelines are available here (in German).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			European Economic Area and ensure that appropriate safeguards are in place in case of cross-border data transfers. 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. 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.	
Germany	Federal Office of Information Security (**BSI**)	15/4/20	**BSI publishes security requirements for health apps** 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. The TR sets out minimum requirements for the safe operation of an application. The TR can be used to meet the requirements of the approval	The press release is available here (only in German). The TR is available here (only in German).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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	**BSI publishes an information package for individuals on secure networking in times of the Covid-19 coronavirus** The BSI announced development of guidance addressing various aspects of the secure use of internet and digital networks during the Covid-19 pandemic. 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: • video calls; • contactless payments; • digital learning and tips for caretakers on safe use of smart devices by children; and • safe video streaming practices.	The press release is available here (only in German). The page with guidance on video conferencing, contactless payments, e-learning and safe streaming is available here (only in German).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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.	
Germany	Federal Office of Information Security (**BSI**)	2/4/20	**BSI issues a brief statement on cybercrime and Covid-19 coronavirus and an update on protection against cyberattacks** The BSI issued a brief statement discussing an increased number of cyberattacks in Germany that target the Covid-19 pandemic. 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 exponential increase in registration of domain names containing pandemic-related keywords and recorded abuses of some of these domains by cyber criminals. The BSI warns users against downloading any Covid-19 apps or installing any software updates from unverified sources. The BSI further refers to its publication providing tips on recognising cyberattacks related to Covid-19 coronavirus and recommendations on protecting against cyberattacks.	The statement of the BSI is available here (only in German). The recommendations of the BSI for protecting against cyberattacks is available here (only in German).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Greece	Hellenic Data Protection Authority (**HDPA**)	15/4/20	**HDPA publishes guidelines on remote working during Covid-19 pandemic** 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. They also point out the heightened privacy expectations of employees working from home. The Guidelines also recommend: • taking measures regarding network access, e.g. using VPN and limiting access rights; • using encryption e.g. on usb sticks; • 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);	The press release is available here. The guidelines are available here. (both only in Greek)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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.	
Greece	Cybercrime Division	3/4/20	**Cybercrime Division issues safe teleworking guide** The safe teleworking guide provides key steps for employers and employees to ensure secure teleworking. More specifically, for employers, the guide recommends: • the adoption of internal policies to manage security incidents; • the encryption of hard drives; • the training of employees in relation to teleworking. In addition, the guide highlights: • the need for specific plans for teleworking; • that employees should avoid using company devices for personal purposes.	The guide is available here (only in Greek).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The guide also recommends two-factor authentication.	
Greece	Ministry of Digital Governance (**MDG**)	20/3/20	**MDG issues guidance on secure internet access** The Greek Ministry of Digital Governance has issued guidance to help people stay safe online. The 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. The guidance also asks citizens to trust official bodies to give them information about Covid-19 and highlights the falsehoods circulating on social media.	The guidance is available here (only in Greek).
Ireland	Irish Data Protection Commission (**Irish DPC**)	3/4/20	**Irish DPC issues guidance on data protection in video-conferencing** 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. 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.	The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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	**Irish DPC issues guidance on staying safe online during the Covid-19 coronavirus pandemic** The Irish DPC published brief guidance for individuals in relation to protecting personal data online during the Covid-19 coronavirus pandemic. 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.	The guidance is available here.
Ireland	Irish Data Protection Commission (**Irish DPC**)	12/3/20	**Irish DPC issues guidance on protecting personal data when working remotely** 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.	The guidance is available here.
Italy	Italian supervisory authority (**Garante**)	28/4/20	**Garante published a note on ransomware in relation to Covid-19 coronavirus** The Garante notes that the extended use of online services and devices connected to internet by individuals due to the Covid-19 coronavirus health	The information note is available here (only in Italian).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			emergency goes along with "digital infection", fuelled by attackers who spread malware for various illegal purposes. One of the most widespread and harmful types of malware is ransomware. The blog post clarifies the following: • 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 ransomware attack to the police and notify Garante if personal data are affected by the attack.	
Netherlands [Reviewed as	Dutch DPA	15/4/20	**Dutch DPA publishes guidance on privacy aspects of video calling apps** In view of increased use of videoconferencing due to remote working in the Covid-19 coronavirus pandemic, the Dutch DPA published a brief guidance	The press release is available here (only in Dutch).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
at 14 May 2020]			note analysing privacy and data protection aspects of 13 commonly used video calling apps and a related table overview. 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. The Dutch DPA recommends choosing a video calling app depending on the following criteria: • the purpose of the call; • the number of intended call participants; • sensitivity of the subject matter of the call in relation to the security of the app. 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. 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.	The high level overview is available here (only in Dutch).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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).	
Netherlands	Dutch DPA	18/3/20	**Dutch DPA issues guidance on secure remote working during Covid-19 coronavirus pandemic** 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: • Secure home working environment: ○ 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).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			○ 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: ○ 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 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- Phishing emails: ○ 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.	
Netherlands	Dutch National Cyber Security Centre (**Dutch NCSC**)	15/3/20	**Dutch NCSC issues guidance for organisations and their employees on cybersecurity aspects of remote working** The Dutch NCSC issued guidance regarding cybersecurity aspects of working from home due to Covid-19 coronavirus measures. The recommendations for organisations include: - 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).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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. In addition, the Dutch NCSC recommends making employees are made 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.	
Poland [Updated as at 4 June 2020]	Polish supervisory authority (**UODO**)	14/5/20	**UODO publishes guidance on video conferencing during Covid-19 coronavirus pandemic** The UODO has published a brief guidance note on the safe use of video conferencing tools and services during the pandemic. Before using a service, the UODO recommendations include: - reviewing the general terms of use and privacy policy of the selected program to check wither video conversations are recorded or stored, how personal data will be used and for which purposes, and which data permissions are asked for (e.g. to allow access to contact list or location); - only installing the official version of an app and running it through an antivirus scan, and verifying that the app has appropriate security measures in place, such as encryption;	The statement is available here (only in Polish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• securing Wi-Fi network with a strong password; • closing all unnecessary applications before sharing the screen with other participants during the the call to prevent unintended information disclosure; • using access codes and PINs when connecting to a conference call. When using the video conference solution, the UODO recommends: • limiting the amount of personal data provided (eg by using a nickname and work email address), enabling password protection and using a different password than for other services; • managing screen sharing options and waiting room options to prevent incidental persons from participating in the call; • using encrypted VPN connection for business-related calls; • never sharing work documents using the public chats; • using the background blur option to prevent callers from seeing personal area; • turning off the microphone and videocamera while logging in to the conference call and turning them on only when needed; after the call, turning off the microphone and video camera and checking that the app is not running in the background.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Poland	Polish supervisory authority (**UODO**)	17/3/20	**UODO issues a Covid-19 coronavirus guidance on working from home** The UODO published a statement providing guidance on measures organisations should take whilst working from home. The statement suggests, amongst other things, that employees should: • 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).
Russian Federation	Federal Service for Supervision of Communications, Information Technology and Mass Media (**Roskomnadzor**)	17/3/20	**Roskomnadzor issues a brief warning about phishing attacks abusing the topic of Covid-19 coronavirus** 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.	The statement is available here (only in Russian).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
Spain [Reviewed as at 18 June 2020]	Spanish supervisory authority (**AEPD**)	7/4/20	**AEPD issues recommendations on the data protection impact of working remotely** 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. 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. 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	The recommendations are available here (only in Spanish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			cloud storage 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**)	12/3/20	**AEPD addresses cybersecurity risks related to Covid-19 coronavirus pandemic** 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. 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.	The blog post is available here (only in Spanish).
Spain	Spanish National Cybersecurity Institute (**INCIBE**)	5/5/20	**INCIBE publishes security recommendations for use of cloud storage services** 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.	The blog post is available here (only in Spanish)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The security recommendations include: • 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; • 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	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			applying secure erasure techniques to remove information that should no longer be stored and ensure cloud service provider policy addresses requirements.	
Spain	Spanish National Cybersecurity Institute (**INCIBE**)	28/4/20	**INCIBE publishes safety recommendations for using video calling apps** INCIBE has published a blog post about secure use of video calling apps. The tips for organisations include the following: • 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; • 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	The blog post is available here (only in Spanish).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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	**INCIBE issues blog post on working remotely** 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 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.	The blog post is available here (only in Spanish).
Switzerland	Swiss Federal Data Protection and Information Commissioner (**FDPIC**)	9/4/20	**FDPIC provides guidance on audio and video conference security** The FDPIC 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.	The press release is available here. The factsheet here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The guidance highlighted the importance of keeping an eye on data protection and information security issues when choosing the software used. In addition the FDPIC emphasised the importance of: • 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. The factsheet recommendations include: • using one time meeting IDs, locking meetings, not sharing meeting IDs publicly and applying a password; • identifying attendees and announce recording; • beware of phishing and verifying meeting invitations from unkown 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;	(both in German)

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- configuring access settings; - setting use regulations and providing guidance to employees; - providing information regarding recordings of employees as required by law.	
Switzerland	Reporting and Analysis Centre for Information Assurance (**MELANI**)	14/3/20	**Swiss MELANI warns about cybercrime attacks using Covid-19 coronavirus emails to spread malware** 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, promptly changing passwords and contacting a specialist support service.	The press release is available here.
UK [Updated as at 18 June 2020]	The Centre for Data Ethics and Innovation (**CDEI**)	15/5/20	**CDEI publishes a blog considering the implications of Covid-19 coronavirus immunitiy certificates for data privacy and cybersecurity** The CDEI blog raises a number of points to consider in relation to antibody immunity certificates, including the ethical implications of use weighed against alternatives such as continued lockdown.	The blog is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The blog highlights potential issues such as whether consent can be relied upon if an individual considers they may only have access to certain facilities with an immunity certificate. The sensitive nature of the personal data involved (health data) increases the risk to privacy, cyber attacks and data misuse but the CDEI considers that appropriate security measures (eg decentralising data, data minimisation and accountability frameworks, fraud resistance) can mitigate risk. Authorisation for use should be clear and care taken regarding identification eg through use of biometrics.	
UK	The UK National Cyber Security Centre (**UK NCSC**) The Cybersecurity and Infrastructure Security Agency (**CISA**) The U.S. Department of Homeland Security (**DHS**)	5/5/20	**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** 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). 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.	The NCSC news report and alert are available here and here. The CISA press release is available here. The CISA alert is available here. The joint advisory is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. The joint advisory report goes on to descibe a number of mitigations including: • 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. The advisory directs reader to a number of existing guidance documents of both the UK NCSC and the US CISA.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			The alert states that the NCSC and CISA will continue to investigate activity linked to APT actors.	
UK	The UK National Cyber Security Centre (**UK NCSC**)	21/4/20 Updated 22/4/20 and 5/5/20	**UK NCSC publishes guidance for organisations on videoconferencing as part of a Cyber Aware campaign** 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. 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: • 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; • 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.	The press release is available here. The guidance is available here. The UK NCSC press releases regarding the SERS are available here and here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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). 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. In particular, the videoconferencing guidance addresses: • 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. When choosing a supplier organisations are encouraged to: • 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	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			independent assessment or audit, and assessment of terms and conditions (such as how provider implements basic security controls, where data is held, and what they can do with it); • 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. When deploying video conferencing the guidance recommends: • using company-wide defaults and controls balancing security and user needs; • setting up single-sign on, integrating use with existing corporate identities; • configuring any password sign-on with the UK NCSC password guidance, including multifactor authentication; • applying least privilege role based access controls;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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; - 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). When communicating with staff guidance recommends: - providing clear user guidance;	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• 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 available) to improve personal privacy when working from a home; • 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.	
UK	UK supervisory authority (**ICO**)	15/4/20	**ICO publishes a blog advising on security of teleconferencing in the context of the Covid-19 coronavirus pandemic** The ICO has published a short blog recognising the challenges of ensuring security of teleconferencing and remote business whilst maintaining convenience. It highlights the advice it can provide to employees on the topic generally and five key questions to ask:	The blog is available here. The Data Protection and Working from Home, What you need to Know

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			• Have you checked the privacy and security settings? ○ 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? ○ 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? ○ Organisations should select a video conferencing platform that matches their policies and employees should check and use the same. • Have you ensured all software is up-to-date? ○ Apply regular software and browser updates.	collection is available here. The security checklist is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- Is this still the right tool for the job? ○ 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. 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. 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. Issues for an employer to consider are set out: *General principles* 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. *Bring your own device (BYOD)* The checklist flags the ICO's comparison to help decide which is the best option for the organisation.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			Cloud storage 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). *Remote desktop* Has the employer limited remote access use as required, disabled default administrator accounts, created specific privileged accounts and ensured account lockouts are in place. The checklist notes that long-term strategies such as VPN access are preferable to short-term fixes. *Remote applications* 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 nad password information. *Email* Has the employer implemented the UK NCSC guidance on defending against phishing attacks, blocked forwarding rules and advsed staff to use corporate email solutions in preference to their own.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
UK	The UK National Cyber Security Centre (**UK NCSC**) The US Department of Homeland Security (**DHS**) The Cybersecurity and Infrastructure Security Agency (**US CISA**)	8/4/20	**UK NCSC and the US CISA publish a joint advisory on malicious cyber activity exploiting the Covid-19 coronavirus pandemic** 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. The advisory notes that APT groups and cybercriminals are actively using the pandemic for commercial gain, deploying various threats, including: • 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. Recommendations for organisations include: • using passwords or "waiting room" features for online meetings to control admittance of participants;	The press statement of the US CISA is available here. The press statement of the UK NCSC is available here. The advisory is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			- 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. The advisory also identifies key online resources published by the UK NCSC and US CISA in relation to mitigating risk online, including: - 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.	
UK	National Cyber Security Centre (**UK NCSC**)	17/3/20	**UK NCSC publishes guidance on Covid-19 coronavirus cybersecurity risks of working from home** The UK NCSC published guidance for companies on managing and mitigating additional cybersecurity risk arising from home working in the context of the	The press release is available here. The guidance is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			Covid-19 coronavirus, particularly due to increased phishing attacks and increased risk of theft. Recommendations include: • 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. 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	Privacy Protection Authority (**PPA**)	23/3/20	**Privacy Protection Authority publishes general guidance on privacy and cybersecurity issues relating to the Covid-19 coronavirus** 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. The PPA confirms that the Israeli Privacy Protection Act 1981 (the **1981 Act**) should not impede health services and other similar organisations processing	The guidance is available here (only in Hebrew).

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			personal information as required in the current emergency, and accepts that there is a public interest in the situation. 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 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. 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. 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
United Arab Emirates (Dubai)	Dubai International Financial Centre (**DIFC**)	26/4/20	**DIFC introduces legislation seeking to limit the impact of Covid-19 coronavirus, including with respect to increased remote working** 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. 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 assists (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 technologies in this context to the extent it outweighs the privacy of employees. Employers must ensure adequate cybersecurity measures in place for remote working (to industry standard). 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. The directive confirms that data subject rights under applicable data protection laws must remain available subject to specific exemptions permissible by law.	The directive is available here (in English and Arabic). The relevant press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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 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 impost 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. 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.	
United Arab Emirates (Dubai)	Dubai Financial Services Authority (**DFSA**)	24/3/20	**Dubai Financial Services Authority issues statement highlighting increased vulnerability of financial institutions to cyberattacks due to Covid-19 coronavirus** 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.	The statement is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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. 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.	
INTERNATIONAL				
International	**G20 ministers for Digital Economy [Updated as at 21 May 2020]**	30/4/20	**G20 Ministers for the Digital Economy commit to working together to leverage digital technology in response the Covid-19 coronavirus pandemic.** Further to the G20 Leader's Extraordinary Summit of 26 March, the Digital Economy ministers held a virtual meeting at which they committed to amongst other things: • 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	The statement is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
			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, human-centric, privacy-respecting research and deployment of digital health technologies; • work together to leverage digital solutions to enable participation in the economy in an 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.	

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
International	**International Criminal Police Organisation (Interpol)**	4/4/20	**Interpol warns healthcare institutions of ransomware attacks during the Covid-19 coronavirus pandemic** 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 key organisations and infrastructure engaged in the virus response. 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. The notice: • highlights the primary mechanism of attack (ransomware via emails) and the need for mitigation; • encourages hospitals and healthcare companies to, amongst other things: ○ regularly update IT systems; ○ backup essential files and store elsewhere; ○ install the latest anti-virus software; ○ use strong passwords.	The press release is available here.

Jurisdictions/ locations (by region and alphabet)	Supervisory authority or regulator	Date	Summary	Source
International	**Financial Action Task Force (FATF)**	1/4/20	**FATF issues statement on Covid-19 and measures to combat illicit financing** FATF President Xiangmin Liu's statement urges governments to work with financial institutions and 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. 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.	The statement is available here.