COVID-19: Cyber and Data Security Legal Checklist

大成 DENTONS

March 19, 2020

The COVID-19 (Coronavirus) outbreak has now been labelled a pandemic by the World Health Organisation (WHO). Many organisations have been taking active measures to contain the virus by asking staff to be vigilant for symptoms and sending staff home in the event of positive tests. In some countries, governments and employers now encourage or mandate remote working and social distancing. Inevitably, these developments trigger cyber and data security considerations, for which we provide a checklist of legal considerations below.

You may also find it useful to read our COVID-19: Data Protection Checklist that covers the broader privacy and data protection issues relating to the collection, processing and sharing of personal data for the purpose of responding to the COVID-19 crisis, as well as our country guides, checklists and guidance on broader legal matters related to COVID-19, such as employment and commercial contracts, which you may find in our COVID-19 (Coronavirus) hub.

Overview of issues and overriding approach

COVID-19 is triggering significant changes in the way in which we work and do business. More remote working, more virtual meetings and conference calls are becoming the norm in the affected parts of Asia, Europe, the US and elsewhere. It may also mean that, because of the significantly higher volumes, your organisation may need to resort to new practices (e.g. using VPN-based technologies to mitigate virtual working capacity issues) and/or engage new business partners to help with confidential business matters and to process confidential information, including personal data (e.g. engaging a new communications or collaborative working platform). At present, it is unclear how temporary or not these changes will be. At the same time, cyber criminals and other malevolent actors will try to make the most out of any opportunity, and COVID-19 is not an exception. Put simply, the COVID-19 crisis is altering the cyber and data security risk landscape.

In adapting their operations to the new reality, organisations have a business interest and a legal obligation to keep systems and data secure by applying appropriate technical and organisational security measures. Neither the public health and other public policy concerns around COVID-19, nor the urgency with which decisions need to be made and changes implemented, provide exemptions from legal obligations to keep systems and data secure. Security defences form the baseline and extend beyond technical controls to organisational measures (policies, processes and contract terms) and people (awareness and training). They must not be diluted as a result of adapting to the COVID-19 outbreak. Beyond statutory and contractual requirements, business partners and corporate customers will likely seek assurances concerning your business continuity arrangements, including regarding cyber and data security, to get comfort that your organisation can continue to service them despite the impact of COVID-19.

The far-reaching impact of the pandemic, the scale of changes required and the urgency in which decisions need to be made, coupled with the underlying public health, public policy and economic wellbeing considerations, mean that organisations should apply legal and business common sense. Cyber and data security are, of course, matters of

great importance, but they need to be balanced against other duties, rights and interests, such as the employer's health and safety obligations, duty of care and responsibility to ensure business resilience and continuity, which are underpinned by public health and economic wellbeing considerations. Clearly, all of these considerations should be factored in when carrying out risk assessments and making decisions about the required security measures. Good intentions, careful thinking (and documentation of the decision-making process), well-orchestrated implementation and, where required, risk mitigation can take you a long way.

Key Dos

- Ensure that the legal and DPO teams work closely with the information security, IT and business continuity teams. Seek external expert support or validation when required.
- Speak with your peer network and external vendors. If you are grappling with a tricky issue (whether technical, organisational or operational), the chances are that someone else is also dealing with it.
- Ensure that the appropriate risk-assessed, technical and organisational security controls are in place. Consider your legal obligations, internal policies, industry standards and the guidance of Computer Security Incident Response Teams (CSIRTs) and centres of excellence, such as the UK NCSC, EU ENISA and the US NIST. See for instance www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19, www.ncsc.gov.uk/guidance/home-working and www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely.
- Consider doing some or all of the following, as appropriate:
  - review your remote/agile working policy/ies, IT acceptable use and Bring Your Own Device (BYOD) policies, and your cyber and data security incident response plan. Adapt them if required;
  - implement security controls in rolling out new IT equipment, onboarding new service providers or sharing data with new parties or in new ways;
  - provide guidance to members of staff as required;
  - provide training, including on any revised policies and practices, where required;
  - raise the workforce's awareness around key issues, such as any changes to policies and processes as a result of COVID-19 and the COVID-specific cybersecurity threats, such as phishing emails, fraudulent websites and malicious apps;
  - refresh guidance on using and accessing sensitive data over potentially unsafe and untrusted Wi-Fi networks;
  - use trusted sources, such as legitimate government websites, for up-to-date, fact-based information about COVID-19.

See the rest of this note for more detail.

- In determining what is appropriate, approach your reviews and risk assessments with a practical mindset and apply legal and business common sense in your analysis. Cyber and data security are critical, but may need to be weighed against other equally, if not more, critical matters.
- If you cannot achieve the desired level of security, mitigate risk to the extent possible, put in place a remediation action plan with defined milestones and approved budget, and implement it as soon as possible.

Key Don'ts

Key Don'ts

- Assume that because of the urgency, the high stakes, the public health and public policy aspects you may lawfully discount cyber and data security controls.
- Forget that cyber and data security is only one of several key considerations at play. Other key considerations, such as the health and safety of your staff, doing the right thing by your customers, ensuring business continuity or protecting public health may need to take priority.
- Be afraid to share or seek insights from others, including your peers, network and external advisers.

Higher levels of remote working

Remote working is of course not new and many organisations already have comprehensive policies, processes and solutions to enable agile, remote and/or home working. However, COVID-19 means that these models now need to be implemented for higher numbers of members of staff, some of whom (including individual employees or entire role categories) will not be used to working in this way, and for an unpredictable period of time.

Now is a good time to review and, if necessary, refresh your remote working policies and processes. It is also a good time to remind members of staff, through awareness messaging, of the controls your organisation has in place to mitigate the cyber and data security risk associated with remote working and what members of staff are expected to do and not do in order to continue working securely away from the office. Ad hoc training may be required for individuals who are not used to working from home, roles that are not normally performed from home and any member of staff who asks for it.

In reviewing your policies, raising awareness and providing training, matters that may require particular attention include:

- how to use secure remote working solutions, such as VPN and desktop virtualisation connectivity solutions and secure sharing/collaborative working solutions, e.g. secure portals and virtual rooms;
- how to deal with problems and receive support, including providing escalation points, contact details, hours of service and emergency procedures;
- the particular risks associated with handling off-site hard-copy documents that contain confidential information or personal data, including around secure disposal;
- the particular risks associated with portable storage devices (such as memory sticks) and their safekeeping and disposal, including the high-risks associated with unencrypted portable devices, the use of which should be prohibited (hopefully your port controls and remote working solutions would not allow their use);
- the particular risks associated with emailing documents containing high-risk data (such as particularly sensitive confidential information, sensitive personal data or high volumes of personal data), and the risk mitigation steps in the exceptional cases that this cannot be avoided (such as encrypting documents, sending passwords by a different medium, double-checking email recipients and calling the intended recipient to confirm safe receipt).

Rolling out more portable IT equipment and relying more on employee-owned devices

To cope with the increased volumes of remote working, your organisation may need to urgently purchase and roll out laptops. Before being delivered to members of staff, these laptops should go through your organisation's usual

security onboarding process, including being encrypted at appropriate levels of encryption.

Similarly, your organisation may need to expand its reliance on allowing members of staff to work using their own devices. This will require purchasing more VPN and desktop virtualisation licences, and ensuring the work-related information is effectively sandboxed. It may also be necessary to review your Bring Your Own Device (BYOD) policy and Acceptable Use Policy (AUP), refresh guidance to members of staff through awareness messaging and provide training to members of staff who are not familiar with the organisation's policy and guidance.

Opportunistic malevolent actions

We already have reports of several threats specifically associated with COVID-19. These range from phishing emails purporting to be from the WHO or keen "customers", to fraudulent websites that have registered coronavirus-related domains (such as covid19.com, coronavirus.com and coronaoutbreakworldmap.com), sometimes with embedded malicious code which imitates legitimate COVID-19 resources, through to malicious apps which, for instance, claim to warn you when coronavirus patients are near you but are actually end user targeted ransomware – see e.g.www.bbc.co.uk/news/technology-51838468, www.forbes.com/sites/mattperez/2020/03/16/coronavirus-scams-watch-out-for-these-efforts-to-exploit-the-pandemic and www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3?r=US&IR=T.

Regarding phishing, given the current levels of concern and the public's thirst for information, there is an even higher risk than usual that one of your members of staff may fall for a COVID-themed phishing email, so an awareness message (whether standalone or part of your broader COVID-19 comms) likely is a good idea. It should:

- raise awareness about COVID-19 related phishing emails, refresh your core messages around phishing in general and address specifically the COVID-19 related phishing attempts;
- provide guidance to members of staff regarding where they can find reliable information and updates about COVID-19 (e.g. your intranet, the WHO website, the UK NHS or other national health service websites);
- provide clear guidance regarding how members of staff should report and deal with phishing emails, especially if they have clicked on any links.

Regarding fraudulent COVID-themed websites, your organisation should be getting updates and/or should be liaising with your cybersecurity, threat intelligence and/or IT service providers that can provide you with lists of domains that are known to be fraudulent, which your organisation may want to blacklist. Similarly, in relation to malicious apps, your organisation's usual controls regarding downloadable apps for corporate equipment should be kept up to date. Raising general staff awareness about fraudulent websites and apps is also advisable.

Sharing data with new business partners and vendors

If as a result of COVID-19 you need to engage new service providers and share with them (including by ways of providing access to) confidential information or personal data, or you need to share such information or data in new ways, carry out appropriate due diligence and ensure you have appropriate controls in place.

In particular, if you are sharing personal data, remember:

- for service providers who act as your data processors, you must carry out pre-contractual data security due

diligence, put an appropriate contract in place (which in the EU should include the GDPR-prescribed processor contract terms), ideally with a minimum security requirements schedule, and have a process in place for auditing them at a later stage;

- for data recipients to whom you provide personal data on a controller-to-controller basis, carry out proportionate due diligence and put essential contract terms in place.

Incident response planning

The virus and the transition to remote working may have an impact on your cyber and data security incident response plan and processes. It is wise to review them and consider if any adaptations are required or updates need to be sent to key incident management and executive stakeholders. Some of the matters that may require attention in the light of COVID-19 include:

- checking if any of the key stakeholders are affected by COVID-19 and may therefore be unavailable when your organisation suffers an incident;
- checking that you have named alternates for every key incident management team member and executive team member;
- checking with your key external service providers (such as your lawyers, first responders, digital forensics providers and insurers) whether COVID-19 has any impact on their ability to service you;
- checking that you have up-to-date contact details and alternative contact details for each key stakeholder;
- checking that your incident response communications protocols and collaborative working infrastructure remain fit for purpose in the light of new working arrangements or making alternative arrangements if required (in which case all relevant stakeholders should be updated).

It is also worth checking if the guidance to members of staff about how they should report a suspected or actual cyber or data security incident needs to be adapted in any way. If it does, then the adaptations should be clearly communicated to the workforce.

Enquiries from customers and business partners

Depending on the line of business that your organisation is in, you may start receiving enquiries from business partners and corporate customers concerning your business continuity planning around COVID-19. These are bound to cover cyber and data security, most likely focusing on the matters addressed above. Therefore, working through the list of matters above will also help you prepare reassuring responses to such enquiries. For instance, questions may include:

- if you have a Business Continuity Plan (BCP) and if you test it;
- whether as part of your BCP testing you have assessed large-scale remote working or flexible working for a prolonged period of time;
- any other measures you may have in place to deal with pandemics/COVID-19 in particular;
- any COVID-19 infection controls that you may have in place;
- the capacity and resilience of your IT infrastructure, including in light of potential increases in cyber attacks,

incidents and breaches given the uncertain environment created by COVID-19;

- whether you have assessed, planned for and/or implemented solutions to mitigate the increased cybersecurity risk and related fraudulent activity risk as a result of COVID-19.

Your Key Contacts

Nick Graham
Partner, London
D +44 20 7320 6907
M +44 7795 618 315
nick.graham@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423
simon.elliott@dentons.com

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com

Antonis Patrikios
Partner, London
D +44 20 7246 7798
M +44 7919 491029
antonis.patrikios@dentons.com

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com