COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2020
Compliance in a work-from-home environment

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Partner & Notary Public at Bristows LLP in London, UK.

The lockdown that was imposed during the COVID-19 pandemic has changed forever the way in which many of us work, and remote access to the office infrastructure and working from home may well be the new normal. However, in the first few weeks of lockdown, many of us were working from home in circumstances that were never anticipated by management—and also without the appropriate technical and organizational structures to manage the information and personal data that we were processing. Now we need to ensure that we manage our obligations regarding data protection, confidentiality, and information security if working from home and from the office have to sit side by side.

Regulatory compliance

Many regulated organizations in the financial and insurance sectors have had difficulty adjusting to working from home, as it makes it harder to supervise traders and staff, monitor for market abuse, and protect client confidentiality. Professions where transactions require identity and authentication to be face-to-face have struggled to adapt to "self-distancing" and also to comply with laws that were created in an age of paper, pen, and ink.

Technology may provide some of the solutions, such as remote monitoring of the use by staff of devices and communication channels, as well as electronic signatures and virtual meetings for documents and authorizations, but these require a reassessment of regulation, risk, and trust.

Information security

In the US, research suggests that successfully changing the culture or attitudes of staff is influenced by the behaviors and communications of senior management.[1] When leaders make cybersecurity a priority and firmly instill it in messages to employees, it sends a very strong signal to the team and also makes it a priority for staff.

The report says, "Here are three things executives can do today to build and reinforce a culture of cybersecurity in their organizations:

1. "**Make cybersecurity a personal priority and 'walk the talk'**: Simple actions like making sure to not click on emails or open links without checking if they are real are examples of cybersecurity hygiene everyone needs to follow."

2. "**Bring cybersecurity into the light**: It's important for leaders to make cybersecurity a personal priority, but it's also important to talk about it often with the organization. To establish a culture of cybersecurity for the whole organization, senior leaders must let everyone know that they are making cybersecurity a personal priority."

3. "**Give extra support to your digital colleagues**: Meet with security and technology teams regularly to learn

and participate in business impact discussions. Listen to their immediate concerns and needs and provide a way to increase support.…Perhaps create cross-functional task forces to address these issues immediately so the business impact is minimized."

In the UK, the National Cyber Security Centre (NCSC) has produced guidance[2] for businesses on how to prepare the organization and staff for working from home, including the use of two-factor authentication for login and the requirement for businesses to produce how-to guidance and webinars to help staff with issues of remote access and the use of conferencing and video services. The NCSC guidance also addresses the need to alert staff to email scams and social engineering as more access is made to online services across a number of devices.

From an information security and cybersecurity point of view, the increased use of social media and the internet give rise to risks surrounding social engineering, phishing, ransomware attacks, and the like; again, guidance needs to be given to staff around awareness of these issues.

Finally, the business needs to consider how it can improve physical and technical security at home for its staff as well as the management of confidential information, including, in particular, manual records and print. While in the office environment, there is usually a control around the disposal of paper and confidential documents, and while it may be harder to manage this within the home environment, the liability still remains.

Privacy and data protection

Organizations that process personal data, whether as a controller or as a processor, are required to comply with applicable law, regardless of where the processing takes place. If working from home on a mass scale were to be implemented by a business today—if it was prudent—it would carry out a data protection impact assessment (DPIA) to consider the risks associated with such a significant change to processing and to employment and information technology practices. The outcome of the DPIA would most likely be an urgent need to implement a number of policies and procedures, to put in place improved security and remote access to the business systems, to issue corporate-controlled devices, and to train staff on their duties in the home working environment.

The reality of the lockdown was that it was neither anticipated by many organizations nor by their staff, and so, almost without warning, the new working arrangements were imposed without a plan—let alone a DPIA!

Data protection authorities around the world have reinforced the fact that during the lockdown and in the period thereafter, in the return to normal, while they may be reasonable about the challenges that organizations face in managing data protection and information security, the laws will still apply.

Businesses need to ensure that they continue to comply with data protection laws, that they put in place and maintain technical and organizational security, and that they provide timely and practical guidance to staff as to how to manage information and personal data while they are being dealt with remotely.

The UK Information Commissioner's Office has produced guidance[3] on what sort of security measures should be put in place when working remotely, how to deal with sharing of information about work colleagues that may have contracted the coronavirus, and how to deal with individuals exercising their data rights during the lockdown.

The European Data Protection Board has also issued guidance[4] on the lawful grounds for processing health data of employees, confirming that consent in the current circumstances is not necessary, as the lawful ground is likely to be public interest or legal necessity. The European Data Protection Board guidance also reminds organizations to ensure that fair processing statements or privacy notices should be updated to address processing of health data in the current situation.

You should revisit your privacy notice to ensure that it covers any new processing activities and any sharing of personal data. Make sure that any contact details you give for data subject requests are still valid and that you have a means of promptly responding to data subject requests or complaints. If time-sensitive communications might come by post, do you have anyone visiting the office to intercept them, and do they know who is responsible for any responses?

If you are carrying out new processing activities in the European Union, have you updated your record of processing activities? How will you manage responses to data subject requests when everyone is working remotely, and how do you control personal data when they are being processed across multiple platforms?

Are you checking the suitability of platforms and video conferencing tools that you are using, and have you complied with your obligations as a controller in respect to data processing terms with processors?

It is worth revisiting the use of DPIAs in respect to the various data-processing activities that the business will carry out during this period, whether it be the sharing of health data regarding staff, the collection of health data regarding visitors, or requiring staff to use new conferencing facilities or chatroom technology. Under the General Data Protection Regulation, DPIAs are mandatory in a number of cases, and so your DPIA process needs to be reviewed.

Working-from-home policy

Some businesses have had a work-from-home policy, but it may have been drafted at a time when working from home was part of the contract of employment for certain staff. Now we have a situation where there is a temporary (we hope) requirement to work from home, and therefore, perhaps there needs to be a specific work-from-home policy put in place. If working from home is to be staggered with working in the office, then this also needs to be addressed.

The home working policy, among other things, will address:

- The required hours of work;
- The expectation that staff should be maintaining an appropriate work-life balance in lockdown;
- The responsibilities for managing office equipment and its return at the end of the work-from-home period;
- Procedures for the purchase by staff of office essentials and the expenses claim process;
- Guidance on how to deal with virtual team meetings and virtual business meetings;
- The requirement for confidentiality in online postings and online discussions, as well as good data and records management; and
- The integration of the work-from-home policy with other compliance policies, including bringing your own device, information security, acceptable use, and social media.

Attention also needs to be given to the interface of the work-from-home policy with flexible working and remote working.

Employees need and expect direction, encouragement, and engagement, and so systems need implementing for regular team meetings, as well as opportunities for “water cooler” moments.

Social media policy

With staff spending so much time out of the office environment, there will be an inevitable increase in the use of social media and digital tools, and that raises risks around the management of confidential information as well as personal data. The business should as much as possible insist that staff use protected devices, but to the extent that they have to use their personal devices and tablets, steps should be taken to ensure that data protection rules are adhered to.

There may be a tendency to spend more time engaging in social media chat, and staff should be reminded that professional standards should be maintained and that when posts are made from the home, there should not be visual items in the background that may cause reputational, brand, or confidentiality challenges.

Data and records management

Another issue that needs to be considered is the risk of the loss of control of data and document conversions. Information may be spread across a number of devices that are remote from the usual central server.

As much as possible, staff should be enabled to remotely access the office servers and platforms using a virtual private network so that data continue to be centralized. However, this may not have been possible in the early days of lockdown, and so control needs to be taken over confidential information and client data on personal tablets and phones, as well as in manual files and print.

When data are imported back into the office system, procedures need to be put in place to ensure that redundant data are deleted and that information on personal devices is also deleted when no longer required. The same applies to print and manual files that need to be disposed of appropriately.

It would be a good time to revisit your data retention and destruction policies, ensure that they address the above concerns, and make sure data retention periods are reflected in the privacy notice and record of processing activities.

Training

Policies and procedures are of no use if employees do not adhere to them and, even worse, if they do not know they exist. It is part of compliance and accountability to ensure that users are trained. Now is as good a time as any to create virtual classroom training and e-learning courses to ensure that you get your compliance standards across to everyone in the business.

It's here to stay

Working from home is here to stay, in addition to remote work, and while we will no doubt also have to come back to the workplace, we need to be aware of the risks of managing information from multiple locations and on multiple devices—in digital or in manual form. Technology is both the sword and the shield, and people are still likely to be the weakest link in the compliance chain.

Takeaways

- Working from home is here to stay, and employers and employees must adapt and adopt.
- Information security and confidentiality are risks that must be managed.
- Data privacy and data protection are critical issues as employers track and monitor employee health.

- Increased use of multiple devices, apps, and social media requires control and training.
- Policies such as working from home, acceptable use, information security, health and safety, and privacy need review.

1 Keri Pearlson and George L. Wrenn, "3 ways leaders can build a stronger security culture," The Enterprisers Project, June 29, 2020, https://red.ht/3180bDh.
2 "Home working: preparing your organisation and staff," National Cyber Security Centre, March 17, 2020, https://bit.ly/325PAFc .
3 "Data protection and working from home: What you need to know," Working from home, Information Commissioner's Office, accessed August 19, 2020, https://bit.ly/2Q4x4aA.
4 "Statement on the processing of personal data in the context of the COVID-19 outbreak," European Data Protection Board, March 20, 2020, https://bit.ly/2EeOcYH.