Working from home — dos and don'ts for controllers

Robert Bond, Partner at Bristows, explains the key considerations for organisations contending with a home-based workforce

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 organisational structures to manage the information and personal data that we were processing. At this point, it is essential that controllers ensure that they manage their obligations regarding data protection, confidentiality and information security properly.

Data protection — general considerations

Supervisory Authorities across the EU have been clear that organisations that process personal data, whether as a controller or as a processor, are required to comply with applicable law, irrespective of where the processing takes place. If organisations intend to implement working from home on a mass scale, they should carry out a Data Protection Impact Assessment ('DPIA') to consider the risks associated with such a significant change to processing and to employment and IT practices. The outcome of such a 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.

Organisations also need to ensure that they put in place and maintain technical and organisational security standards, and provide timely and practical guidance to staff as to how to manage information and personal data whilst they are being dealt with remotely from the workplace. The UK's Information Commissioner's Office has produced guidance 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 Covid-19 and how to deal with individuals exercising their data rights during the lockdown (see 'Working from home – security checklists for employers', 'Workplace testing – guidance for employers', and 'Data protection and coronavirus — what you need to know', all via the ICO's data protection and coronavirus information hub. (www.ico.org.uk/global/data-protection-and-coronavirus-information-hub/)

The European Data Protection Board ('EDPB') has also issued guidance 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 EDPB guidance also reminds organisations to ensure that fair processing statements or privacy notices should be updated to address processing of health data in the current situation.

Organisations should revisit their privacy notices to ensure that they are updated to cover any new processing activities and any sharing of personal data, and that any contact details given for data subject requests are still valid (i.e. there is a means of promptly responding to data subject requests or complaints). They should also confirm that if time sensitive communications come by post, there is someone at the office to intercept them, and direct them to those responsible for responding.

If carrying out new processing activities, the organisation's Record of Processing Activities should be updated. Organisations should establish how responses to data subject requests are managed when everyone is working remotely, and how personal data are controlled when they are being processed across multiple platforms. They also need to check the suitability of platforms and video conference tools, and comply with their obligations as a controller in respect of data processing terms with processors.

It is worth revisiting the use of DPIAs in respect of the various data processing activities that the organisation 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 chat room technology.

Information Security

The UK's National Cyber Security Centre ('NCSC') has produced guidance for organisations on how to prepare staff for working from home, which 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.

The NCSC recommends that organisations consider the following:

- introducing and communicating sensible and pragmatic security arrangements that support staff whilst using remote IT systems;
- providing simple 'how-to' guides for staff;
- encrypting laptops and installing a system to track and delete data from tablets and phones remotely if they are stolen;
- controlling business data being used on shared home equipment;
- moving to two-factor authentication;
- maintaining confidentiality standards in communications;
- producing guidance promoting awareness of the increased risks surrounding social engineering, phishing, ransomware attacks; and
- improving physical and technical security at home for staff, including ensuring that personal data disposal can be carried out properly.

Working from home policies

Whilst many organisations probably already have a home working policy, this may have been drafted at a time when working from home was part of the contract of employment for certain staff. Given the situation now, there needs to be a specific home working policy. If working from home is to be staggered with working in the office, then this also needs to be addressed.

Such a policy should cover:

- required hours of work;
- the expectation that staff should be maintaining an appropriate work versus life balance in the lockdown;
- the responsibilities for managing office equipment and its return at the end of the home working requirements;
- procedures for the purchase by staff of office essentials and the expenses claim process;
- guidance on how to deal with virtual teams 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 home working policy with other compliance policies including Bring Your Own Device, information security, acceptable use and social media.

Social media policies

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. This raises risks around the management of personal data. Organisations 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 to ensure that professional standards are maintained. Where postings are made from the home environment, there should not be visual items in the background that may cause reputational or brand or create confidentiality challenges.

Data and records management

As far as possible, staff should be enabled to remotely access the office servers and platforms using a Virtual Private Network (VPN), so that data continue to be centralised. As this may not have been possible during the early days of lockdown, it is paramount that organisations now have control over business confidential information and client data on personal tablets and phones, or 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. Organisations should revisit their Data Retention and Destruction Policies to ensure that they address the above concerns, and that data retention periods are reflected in the privacy notice and Record of Processing Activities.

Training

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

Conclusion

Working from home and remote working is here to stay. We need to ensure that our technical and organisational systems and procedures are adapted to meet the risks and challenges as well as the opportunities that come with this new work environment. We also need to recognise the human elements, as well and develop support and training for our staff to protect both them and the business.

Robert Bond
Bristows
robert.bond@bristows.com