CLIENT BRIEFING

Coronavirus – Working From Home – Five Things for Businesses to Consider

26 March 2020

CONTENT

INTRODUCTION

Asking employees to work remotely can be difficult, especially for organizations that don't have remote work already embedded in their culture and may not have the necessary systems and protocols in place to support it.

Managing remote workers creates a number of critical challenges for any organization, but especially professional and financial services firms, where protecting client data and sensitive commercial information is paramount. The stakes are high and getting this wrong may result in costly litigation, reputational damage, and fines from regulators.

Many organizations, even those who prepared amply for the implementation of the General Data Protection Regulation (GDPR) in 2018, are now finding their data protection policies being tested in unexpected ways. Unless policies are adequately enforced or rapidly adapted to the current circumstances, data leaks remain a serious risk.

Here are some points to consider:

1. Cybersecurity

While most business have secure internet connections in the office, many will now find themselves with employees logging on from home via personal, unsecured wi-fi systems where the password may be simply "password" rather than through a secure (and monitored) corporate network that enforces password standard policies, firewalls, and so on.

Employers should provide IT support and guidance to allow workers to secure their home computer systems to protect documents sent and conversations had over email, virtual conference calls, and voice calls.

2. Data Protection

There are significant data protection implications arising from legislation including the GDPR and the UK Data Protection Act 2018 (DPA 2018). The US doesn't have federal-level data security laws yet, but GDPR applies globally to protect EU residents and is an excellent standard to follow.

Businesses with remote workers should assess whether staff are using home devices to access critical company data or client documentation. If so, review data protection policies and educate staff to prevent data leakage and personal data from being stored (and backed up) on home devices.

Employers will need to take appropriate technical and organizational measures against the processing of data that identifies an individual's personal information and to protect against the accidental loss or destruction of data.

Processing is widely defined to include obtaining, storing, viewing, holding, recording, transmitting, or destroying information or data, or carrying out any operation or set of operations on the information or data.

Leakage of personal data may take many forms, from inadvertent back-ups on home IT devices to using home scanners (leaving a digital image of the document stored locally), and printing papers at home (which can result in information ending up in the trash rather than a shredder). It is also worth considering that any future discovery process, should litigation arise, is far more challenging when personal devices are involved.

3. Email and paper mail

Companies should actively monitor emails to ensure that work accounts are being used and personal accounts are not. Most devices allow multiple email accounts to be accessed via the same application or platform; this should be discouraged.

Companies should also consider what policies to put in place to deal with paper mail. With lockdowns of cities becoming more common, it may not be possible, or advisable, to have staff attend premises to check for mail. Redirecting mail or having employees use home addresses for correspondence on a temporary basis may help, but issues regarding audit trails and the safe disposal of paper documents will need to be addressed.

4. Communication

One of the biggest challenges in managing remote workers is ensuring effective communication. With team members spread out across multiple locations, coordinating work hours to schedule online meetings isn't easy. This can cause confusion that slows progress and delays the completion of projects. In addition, in the UK, employers still owe a duty of care to those working from home, and communication may be required for the employer to discharge its responsibilities properly.

5. Equipment: the use and monitoring of communications systems

Employers need to consider what equipment will be required by a home-worker, who will provide and pay for it, and who can have access to it.

If a home-worker will use computer equipment supplied by the employer and will have access to the internet and/or email facilities, the employer will need to consider applying any systems it has in place for policing the use to which the homeworker might put the facilities at their disposal. Employers will also need to satisfy themselves that the risk of a data security breach is low.

Employers can address many issues by implementing a clear and thorough IT and telecommunications policy. This may include measures to protect the confidentiality of electronic information; to monitor the use of email and the internet and the extent to which (if at all) either may be used on a personal basis; to monitor the use of other electronic communications; and to clarify what will be considered inappropriate use. The policy should include clear information about the types of monitoring an employer may undertake, and

who will have access to such information. Employers should also consider whether the policy captures issues that typically affect home-workers. For example, does the policy cover appropriate use of social media, and an employee's obligations to protect their employer's reputation, even from home?

A good policy may also include:

- Tailoring standard employment contract clauses to encompass home-working;
- Strengthening measures to protect confidential information and personal data;
- Reviewing the health and safety implications of home-working arrangements, including carrying out a risk assessment;
- Deciding what special equipment, if any, should be provided;
- Considering whether any special planning or insurance arrangements are required;
- Deciding what arrangements should be made for the management and supervision of certain types of homeworkers; and
- Identifying the tax consequences of homeworking.

While it is too soon to draw any conclusions about the possible long-term effects of the coronavirus pandemic on working patterns, it is clear that the way we work could change significantly in the future. Now is the time for companies to test and implement policies that will ensure that they have the flexibility and requisite security to adapt to an uncertain working environment.

Should you have any questions about the topics covered in this article, please get in touch with Rooney Nimmo partner, Edward Sloan or your usual Rooney Nimmo contact.

CONTACT

Edward Sloan

Partner
Tel: +44 (0)7715 380 367
edward.sloan@rooneynimmo.co.uk

rooneynimmo.com

Edinburgh • London • New York • San Francisco ◆ Beijing ◆ Shenzhen ◆ Hong Kong