lindsays

Covid-19 : Guidance on data protection matters for businesses with homeworking employees

The current social distancing measures mean the majority of businesses have faced and implemented a quick transition to homeworking for their employees. One of the significant challenges this presents is how to comply with the GDPR and data protection legislation outwith the office.

Data protection legislation has the same parameters, whether your employees are working in the office or at home. The data controller remains responsible for data protection compliance. For more information on what this involves, click here.

Homeworking can often present new challenges to data privacy for businesses. Here are some practical tips to help you consider how to keep data protection compliant:

Make your employees aware of their data protection responsibilities

It is important that employees understand the underlying concepts of the data protection legislation and what is expected of them. For some employees, homeworking might mean their role has changed slightly and they have access to more data than they would in the office.

It might be helpful to arrange refresher data protection training.

Ensure your policies are up to date

You should have clear and available data protection policies for your employees. These should cover the data protection principles you expect employees to follow, your data retention policy, how to respond to any data subject requests and any other data protection matters arising.

If employees are using personal devices to work from home, you should have a Devices Policy in place to regulate the use, management and security of any devices that may hold business data.

You should also consider your Privacy Notices and whether any changes are required to reflect any changes to how you are currently working.

Review your security measures

It's particularly important that you ensure your security measures are robust when employees are working from home.

Virtual security - whether your employees are using business devices or personal devices, you should ensure they have appropriate security software and are encouraged to change their password regularly. You should ensure your employees are alert to any phishing or hacking attempts and duly report these.

Physical security - homeworking might mean that employees need to access hard copy documents (though you should try to avoid this if possible). While you might have robust confidential waste procedures in the office, it's important that security measures are considered for employees at home as well. Sensitive documents should still be properly held (within locked cupboards or filing cabinets) and securely destroyed in due course.

Shared spaces – unlike in the office, employees working from home may be sharing space with family or housemates who are not employees of the same business and should not have access to any business or other confidential information. Employees should be advised to be mindful of this, and to consider their security and confidentiality obligations.

Keep managing any data breaches

Any breach of security, whether in the office or at home, should still be carefully considered in case it constitutes a data breach. Employees should be encouraged to report as soon as possible any issues or concerns to whoever is responsible for data protection compliance in your organisation.

You should try to mitigate the effects of any data breach as quickly as you can and evaluate the consequences of the breach. If the breach is reportable, the usual reporting deadlines apply. For more advice on reporting data breaches, click here.

For further guidance and support, you can get in touch with your usual contact at Lindsays or:

Nimarta Cheema, Senior Solicitor in Corporate & Technology
nimartacheema@lindsays.co.uk
0131 656 5686

Guidance correct as at 19 May 2020
Please contact a member of the Corporate & Technology team for up-to-date or specific advice