COVID-19 REMOTE WORKING TIPS

Working remotely brings increased risks relating to data protection and information security. The DPO Centre has launched 19 best practice tips to keep you and your organisation safe and tackle the data protection challenges you may face.

1 ALWAYS LOCK YOUR SCREEN WHEN AWAY FROM YOUR DEVICE WINDOWS: ⊞ + L MAC: ⌘ + ^ + Q

Data can be inadvertently breached when you leave devices logged in. The solution requires only a few simple keystrokes.

2 HANDLING WORK DOCUMENTS AT HOME? USE A CROSS CUT SHREDDER (YOUR KIDS WILL LOVE IT)

The DIN 66399 Level 3 is appropriate for "standard" document shredding. This is defined as, "data media with sensitive and confidential data as well as personal data to high protection requirements". This is therefore appropriate as a minimum level in order to comply with the GDPR. When shredding to Level 3 standard, the maximum shredded particle size at this level would be 320mm2.

3 AFTER INSTALLING UPDATES, MAKE SURE YOU REBOOT

Installing updates is of course vital, but did you know they don't take effect until the device has been rebooted? Make a point of rebooting regularly.

4 ENCRYPT YOUR FILES 'AT REST'. TURN ON ENCRYPTION

When your device is locked, it is very difficult to access the data on the device, however the storage device can just be removed, connected to an alternative device and the data read. When encrypted 'at rest', the data is unreadable. If you use a Windows PC, activate Bitlocker or for a Mac, use FileVault. Both are free with all recent versions.

5 DOES YOUR ORGANISATION HAVE A BRING YOUR OWN DEVICE (BYOD) POLICY? HAVE YOU READ IT?

Many of the tips we are providing here will be in this policy, but with the added benefit of them being specific to your organisation. Check your company handbook or request a copy from your data protection lead.

6 ENSURE YOUR HOME ROUTER IS NOT USING THE DEFAULT ADMINISTRATOR PASSWORD AND IP ADDRESS

Many domestic routers including those from Linksys and Cisco use default administrator passwords such as "admin" or "cisco". Worse still, the admin interface can be accessed using the default IP address (i.e. 192.168.1.1). This makes it easy for anyone within range of your router to login and change your DNS settings, meaning that all your browsing activity (including passwords entered) can be rerouted and recorded without you being aware. Change your default settings now.

7 IF ASKED TO ENTER BANK DETAILS OR PASSWORD AFTER CLICKING A LINK IN AN EMAIL, DON'T

No matter how convincing and genuine an email looks, if you are asked to enter your bank details (for say a furlough payment, tax refund or that government grant you are waiting for) or to confirm your password (as they need you to confirm your identity), in all likelihood it is a scam. Call the company using the number off their website (not the email you've received) and confirm.

8 BE VIGILANT WHEN RECEIVING CALLS FROM UNKNOWN SOURCES

If personal or sensitive data is requested from an unknown caller, even if they say they are from your broadband provider, IT or HR department, HMRC or the Police etc, verify the caller's identity before providing any information. Ideally, call them back (not using a number they provide) and ask them to confirm something about you that is not in the public domain.

9 USE STRONG AND VARIED PASSWORDS, BUT DON'T WRITE THEM DOWN, USE A PASSWORD MANAGEMENT TOOL

OK, so you hear this one all the time, but did you know an 8 character lower case password can be defeated (by a normal PC) in 0.007 seconds? Make that password 12 characters using upper and lower case, numbers and special characters and it becomes 559 years.

Head Office
The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

Registered Office
Suffolk Enterprise Centre
Felaw Street
Ipswich IP2 8SJ

Dublin Office
Alexandra House
3 Ballsbridge Park
Dublin D04 C7H2 Ireland

Contact Us
0203 797 1289
hello@dpocentre.com
www.dpocentre.com

Outsourced Data Protection

10 WHERE POSSIBLE, DON'T CONNECT TO PUBLIC WIFI, USE A HOTSPOT ON YOUR MOBILE INSTEAD

So, we're not using coffee shops and trains so much at the moment, but when you do, a hotspot on your phone is more secure. WiFi "Pineapple" devices are freely available to buy from Amazon. These devices mimic the free WiFi service such that your device connects to them automatically, meaning all your browsing traffic is rerouted and recorded (including any passwords entered) without you being aware.

11 FIND OUT WHO TO CONTACT IN YOUR ORGANISATION IF YOU SUFFER A PERSONAL DATA BREACH AT HOME

Data breach reporting requirements remain, whether it happens at home or work. Understand your breach reporting process and given your DPO or the person you normally report breaches to may no longer be at work, ensure you are aware of who has adopted this responsibility.

12 WORKING ON PAPER RECORDS CONTAINING SENSITIVE COMPANY DATA? STORE IT IN LOCKABLE STORAGE BOX

Your teenage kids may not be inclined to sell the personal data from the paper records you are processing at home to the highest bidder on the dark web, but it does not change the fact that they, or any other person in your household, are not authorised to view company personal data. Paper documents containing normal personal data should be tidied away out of sight, however sensitive 'special category' data should be stored in a lockable storage box.

13 ASK YOUR ORGANISATION TO TEMPORARILY DISABLE YOUR ACCESS TO UNUSED SYSTEMS

If you have been furloughed or don't currently need access to your organisation's systems (i.e. HR, CRM, file server etc), then ask for your access to be temporarily revoked. This will further protect your organisation's system, should your home PC be compromised by malware or bad actors.

14 ENABLE LOCATION SERVICES AND REMOTE WIPE ON MOBILE DEVICES

Lost or stolen devices pose a serious breach risk if they store or provide access to your organisation's personal data. Enabling location and remote wipe services from your iCloud or Google account provides you with an additional level of protection to maintain remote control over the device. Have you checked to see if it's enabled recently?

15 ENSURE ALL YOUR DEVICES HAVE ACCESS CONTROL ENABLED AND THEY AUTO LOCK AFTER INACTIVITY

Screen locks provide your devices with a fundamental layer of security, which should be mandatory when used to process personal data. You should always lock your device before leaving it unattended, even at home. Screen locks can be setup to use a PIN, facial recognition or fingerprints. Does your screen lock?

16 IF YOUR TELEPHONE CONVERSATIONS INVOLVE THE EXCHANGE OF PERSONAL DATA, MAKE SURE YOU CANNOT BE OVERHEARD

Data protection is not just about digital and paper records, it also includes what you say. If you are having conversations at home where personal data is being exchanged, or you are discussing an individual, close the door and ideally, switch off your Google Home and Amazon Alexa type voice assistant devices.

17 DON'T SHARE ACCESS TO WORK DEVICES WITH YOUR FAMILY

The kids or your other half may enjoy having a further device to use, but if the device was provided by your organisation, then it should only be used for work purposes. Recreational use by other members of your household will significantly increase the risk of compromise through unauthorised access and the inadvertent installation of malware, so do not share the device's login details.

18 IDEALLY, DON'T SAVE WORK FILES LOCALLY, BUT IF YOU HAVE TO, DON'T FORGET TO CREATE A BACKUP

There is a difficult balance to make. Data security implies you should take multiple backups, but data protection requires minimisation. If the only copy of personal data is lost or becomes irretrievable, then this is a breach. Wherever possible, personal data should remain stored in your organisation's facilities (network server, cloud storage, apps etc), but if it is only practical to work on personal data locally, store a backup on a separate device to protect against loss.

19 REMEMBER, IF THE ONLINE SERVICE IS FREE, YOU ARE THE PRODUCT BEING SOLD

Nothing is ever truly free, especially online. It costs millions to create, host and maintain online services such as games, mobile apps and online platforms. If they are free to download or use, then it is highly likely their income is derived from selling your personal data, including your preferences, opinions, location, actions or inactions, browsing or conversation history, etc. Consider carefully what you sign up for.

Head Office
The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

Registered Office
Suffolk Enterprise Centre
Felaw Street
Ipswich IP2 8SJ

Dublin Office
Alexandra House
3 Ballsbridge Park
Dublin D04 C7H2 Ireland

Contact Us
0203 797 1289
hello@dpocentre.com
www.dpocentre.com

Outsourced Data Protection