Working from Home: Cybersecurity & Data Protection Considerations

Dr Emma Grech and Dr Naomi Schembri

02 May 2020

Adapting to a New Reality

Aside from the worldwide humanitarian crisis that the spread of the COVID-19 pandemic has brought along with it in a matter of weeks, the various measures announced by governments across the globe in efforts to safeguard their populations' health from the virus have significantly disrupted the manner in which business organisations operate on a day-to-day basis. As a result, a great number of entities have had to be amenable to making a number of important changes to the manner in which they would normally conduct their businesses in an attempt to stay afloat whilst easing themselves into this new – albeit still emerging – reality.

The Transition to a 'Work from Home' Environment

A major decision organisations have had to make was whether to close down their businesses until further notice or whether to continue operating on a remote basis. Opting for the latter meant a sudden relocation of (possibly) an entire workforce from a previously office-bound environment to a new home set-up. Although such transition might, at face value, seem relatively simple, there are a number of important considerations which must be taken into account by any affected entity when implementing the required changes. In particular, the affected entity must consider a possible update to its IT and information security systems and the introduction – or enhancement – of more robust internal measures, and this in order to guarantee an adequate level of protection to any personal data stored on its systems when this is now being accessed remotely.

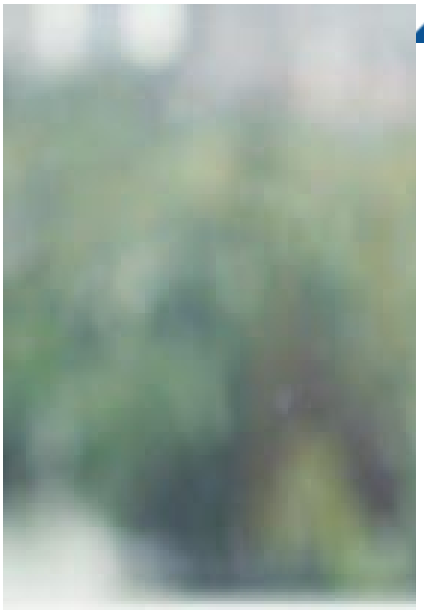
Image by: pressfoto/Freepik

Unfortunately, however, it is becoming ever-more evident that, in critical situations such as the one being faced at present, cybersecurity and data protection considerations end up being overlooked or pushed aside by a large number of businesses. The economic, industrial and societal strains brought about by this unprecedented wave of change might lead to the adoption of a cost-cutting mentality where the investment of capital in one's IT and information security infrastructures is seen as an unnecessary burden. In truth, however, this mentality will probably result in very expensive longer-term consequences, as the relevant entity would be left exposed to a myriad of problems, including significant financial hardships due to the hefty fines that could be imposed by data protection authorities; but not only, as loss of clients and reputational damage may most likely follow. This might even end up crippling or, in the worst scenarios, completely destroying the afflicted entity's business operations.

Cybersecurity and the Protection of Data: Employer's Duties

It is known that cyber-criminals take advantage of crises. In March 2020, Europol released a report on the manner in which cyber-criminals are using the COVID-19 crisis in carrying out social engineering attacks. As the majority of people struggle to find their feet and adapt to the new circumstances, cyber-criminals circulate phishing emails, scams, fake websites, fake profiles, viruses and malware in an attempt to infiltrate systems and private databases. This is largely done through the exploitation of IT and information security vulnerabilities which a business organisation, in the rush to implement new changes to its *modus operandi,*and, or to cut costs, would have inadvertently – or negligently – left unaddressed.

Since the outbreak of the virus, we have in fact been witnessing a sudden increase in cyber-attacks, both internationally and locally. The result is an increase in the fines that are being imposed on entities for the infringement of various data protection obligations incumbent upon them in terms of the applicable data protection laws, in particular, the General Data Protection Regulation (EU 2016/679) (the "GDPR"). The strength of an organisation's IT and information security systems and the protection of data therefore become fundamental considerations for all entities that seek to



operate through a remote workforce. It is essential for these entities to identify their weakest security points and take all the appropriate actions in addressing and mitigating any existing risk of cyber-attacks and resultant data breaches.

The starting point is to conduct a thorough **risk assessment** of the entity's own systems, principally to identify the new challenges which the entity is or shall be facing as a result of the shift to a remote environment, and, subsequently, to assess if it is sufficiently equipped to cater for such challenges. It is not necessarily the case that the findings thereof will require a major upheaval, especially, of course, if the particular entity already offered the possibility of remote work to its employees. That said, the approach and measures required would be specific to each and every entity as these would greatly depend on the nature of the business operations, IT infrastructure, current practices, policies, as well as the organisational and technical security measures which are already in place. It is recommended that employers cater for and address the results of the risk assessment through an **effective, workable and practical business continuity plan**.

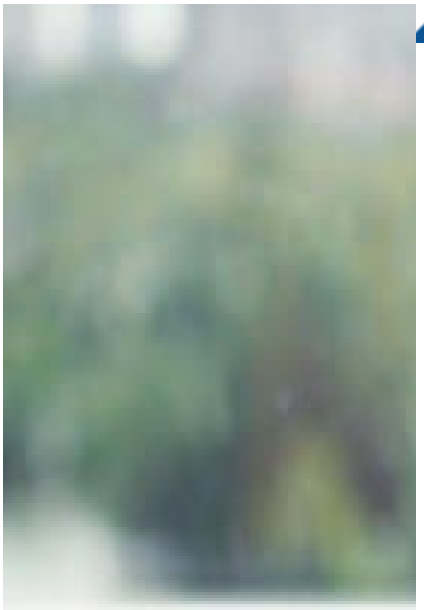
Amongst the key considerations which should feature in said plan, the below should be at the forefront:

- **The use of virtual private networks (VPN) by employers so as to allow their employees to remotely access the internal systems of the workplace**. This is perceived to be one of the most secure ways in which internal databases and servers may be accessed externally. Employers are to constantly practice patching and ensure that their VPN system is kept updated to avoid any unauthorised infiltration into its systems and possible data breaches.
- **Employing adequate endpoint security to all wireless devices being used by the entity's employees to access internal networks, and this in line with the applicable data security standards**. Endpoint security mainly requires the use of strong passwords, up-to-date firewalls and antivirus software, encryption of data, the prevention of unauthorised downloads and use of applications and the limitation of external storage devices implemented by end-users.

- **Employers are to ensure that they document and address all vulnerabilities in the cooperative platforms and video-conferencing applications which may be used by their employees, and adopt the necessary security measures to mitigate any risks that may be posed by the use of such platforms**. This may require the prior testing thereof on which clear instructions should then be passed onto employees as to which applications they are allowed to use to the exclusion of others.
- **Continual educating and training of employees** is a must in these scenarios. Entities should never presume that their employees have sufficient knowledge on how to securely carry out their tasks remotely. Employers should therefore take care to supply their workforce with user-friendly policies, protocols and any other required materials which are to continue being updated as necessary from time to time. Any such information shall also aim to provide employees with directions on what procedures they should follow in an event of a cyber-attack or data breach, whilst at the same time increasing the employees' overall awareness as to the cybersecurity risks being faced by the entity and their obligations under the applicable data protection legislation.
- **Meticulously following and adhering to the employer's data protection obligations, and this as required by the GDPR, the Data Protection Act (Cap. 586 of the Laws of Malta) (the "DPA"), and all applicable data protection rules and regulations generally.** Light is being thrust onto the Telework National Standard Order (Subsidiary Legislation 452.104 of the Laws of Malta), specifically with reference to the data protection obligations of employers when engaging in "telework" (as defined therein).

In terms of these regulations, employers have data protection obligations specific to the telework context as they are required to implement appropriate security measures, particularly with regard to software, to ensure the protection of data when this is being used by the employees whilst performing their duties.

Additionally, employers are required to specifically inform their workforce of the provisions of the DPA and of any security measures undertaken to safeguard the protection of data when being processed from a remote environment, including any restrictions on the use of IT devices, internet or other IT



equipment intended to be used for purposes of work, as well as any existing sanctions in the event of non-compliance with such obligations.

Cybersecurity and the Protection of Data: Employee's Duties

Although the onus of assessing and mitigating cybersecurity and data protection risks rests mainly with employers, employees are not to underestimate the importance of their actions in limiting the risks and effects of a potential cyber-attack as well as in keeping data secure when working from home. One 'mis-click' from an employee can lead to the destruction of an entire business.

Employees shall, therefore, **familiarise themselves with basic IT hygiene practices**, such as, by way of example:

1. limiting the use of work-devices for work-related purposes only. Browsing for leisure, shopping or the downloading of movies is to take place on personal devices;
2. password-protecting their work laptops, phones and other devices;
3. ensuring that they are making use of a secure and password-protected internet connection;
4. using basic firewalls and antiviruses on all devices;
5. avoiding connecting external storage devices, such as USBs, to work devices when these are also used for personal purposes;
6. maintaining the confidentiality of data from any relatives or cohabitants; and
7. being aware of suspicious emails generally.

The teleworking employee is also obliged, in terms of Subsidiary Legislation 452.104, already mentioned, to **abide by the provisions of the DPA** in ensuring the correct processing of personal data, as well as to **follow any measures communicated by the employer** as may be adopted internally to ensure the security of IT systems and infrastructure.

A Future Powered by Technology

Cybersecurity and data protection go hand-in-hand and their relevance acquires even more prominence in the context of the present and unsettling scenario. The adoption of adequate security measures should no longer be perceived as an option, but rather as a must. The reality of such a statement will become more pertinent as the world continues moving into an innovative era powered by technology, where entities shall eventually start considering the long-term adoption of remote work beyond the trying days of the present pandemic.

Indeed, it is unlikely that organisations will go back doing business in exactly the way they were accustomed to before the *novel coronavirus* outbreak, as remote work will most likely become the order of the day for a number of enterprises. Consequently, efforts and investments made by business organisations to ascertain the fitness and propriety of their infrastructures against the COVID-19 backdrop today are not only bound to assist entities in navigating the current circumstances, but are also intended to set them up for the 'new normal' that mankind has only just begun to experience.

For more information on how we may assist with any of your data protection needs, please contact:

Dr. Emma Grech, Partner –
emma.grech@thecitylegal.com
Dr. Naomi Schembri, Associate –
naomi.schembri@thecitylegal.com

A: CITY LEGAL, Britannia House, Level 1, Old Bakery Street, Valletta, VLT1450, MALTA

E: mail@thecitylegal.com
W: www.thecitylegal.com
T: +356 2744 1120/1