Data Protection and Remote Working

April 23, 2021

There hasn't been an organisation within the charity, community and voluntary sector that hasn't been disrupted as a result of Covid-19 and it looks like this disruption is set to continue for some time yet. For most of us, it has now been well over a year since employees have been in their normal place of work.

It would have been inconceivable this time last year to think that so many of us would still be remote working. But if we've learned anything over the past 14 months, it's that all organisations are far more adaptable and versatile than we previously thought.

Covid-19 has accelerated organisational transformation at an unbelievable pace. But employers and employees have demonstrated resilience and agility in how to approach work. These new ways of working have put a spotlight on the importance of effective systems and technology in order to maintain a functional and productive workforce. But the importance of data protection whilst working remotely has not always been a primary focus and organisations should ensure that it is always to the fore when so many employees are continuing to work outside the office.

Data Accessibility

The need to ensure personal data is safe when working remotely from home should be an on-going process. The need to have in place a functional remote working policy that captures the requirements necessary for data protection purposes is extremely important.

Key to safeguarding your organisation is management of remote functionality, such as, providing guidelines on your operational model and data accessibility. While a remote working policy should set out clear guidelines on the operation of devices, proper use of emails and the security and confidentiality of paper records, data accessibility practices should also be clearly defined.

With an increased demand of managing issues that arise whilst remote working, data accessibility which is not planned out in a manner that addresses the requirements of your organisation will also become an issue. Now is the time to revisit that area and apply a set of rules that identifies the accessibility requirements of each individual employee. On the premise that no one employee should have access to all files contained within your infrastructure, then it is important to review the access deemed necessary for each role and department function.

Compliance with GDPR Regulations has not diminished by virtue of the pandemic, but rather it places organisations in a unique environment that necessitates employers within the community, charity and not-for-profit sector to adapt and reinforce the compliance requirements. This means that cloud and network access must be fit for purpose in view of the remote working environment and the challenges presented by remote working practices. Procedures should be in place that require employees to use strong password controls, to continuously update login credentials, to enable two factor authentication and to apply strong encryption on devices when working remotely from home.

The biggest change stemming from remote working environments has been the increased and mostly constant use of video conferencing. The Data Protection Commission has set out useful guidance on safe and secure use of video-conferencing arrangements to ensure an adequate standard of data protection is applied, all of which are set out below for your information.

Data Protection Tips for Organisations and Video Conferencing[1]

Employees should utilise the organisations contracted service providers for work related communications and employers should ensure they are happy with the privacy and security features of the services being used by employees. Ad-hoc use of apps or services by individuals should not be encouraged.

Employers should ensure that employees use work accounts, email addresses, phone numbers, etc., where possible, for work-related video conferencing, to avoid the unnecessary collection of their personal contact or social media details.

Employers should have in place organisational policies and guidelines that are clear, understandable, and up to date to those using video conferencing. This will enable employees to be responsible for knowing the rules that should be followed and steps that should be taken to minimise data protection risks. This should include information on the controls the services provide and that are available to them to protect their security, data, and communications. Employers should advise employees to implement appropriate security controls such as access controls (such as multi-factor authentication and strong unique passwords) and limit use and data sharing to what is necessary.

Where video-conferencing services need to be used for organisational reasons, employers should have a consistent policy regarding which services are used and how, and offer access through VPN or remote network access where possible.

Employers should ensure that employees are advised to avoid sharing organisational data, document locations or hyperlinks in any shared 'chat' facility that may be public as these may be processed by the service or device in unsafe ways.

Conclusion

Though there is a promised return to some form of normality with the continuation of the vaccination programme, remote or hybrid working practices will continue for many organisations. This is why regular reviews of the application of data protection regulations should remain a priority and when practised regularly, will mitigate any potential risks of breaches to the GDPR regulations.

Disclaimer – The information in this section is provided for reference purposes only to assist Employers with the government protocols and guidance from relevant statutory bodies and must be read in that context and should not be used for or interpreted as a legal definition of any of the information provided. Some of the information provided is per information published on the websites at www.gov.ie. Professional advice should always be sought before making any such decisions, April 13, 2021.

[1] www.dataprotection.ie