adare
human resource management

Update on Coronavirus

Data Protection & Remote Working

With the restrictions announced by Government on Friday last now extended to May 5, 2020, Employers and Employees alike face three additional weeks of working remotely from home to mitigate and prevent the spread of COVID-19.

At Adare Human Resource Management we have previously discussed additional measures that should be taken by Organisations to ensure personal data is safe when working remotely from home. However, with the extension of the restrictions now in place it bears relevance to reiterate the importance of having in place a functional remote working policy that captures the requirements necessary for data protection purposes. Key to safeguarding your business or Organisation is management of remote functionality such as guidelines on your operational model and data accessibility. While the remote working policy will 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.

The rush to move to remote working may mean that data accessibility was not planned out in a manner that addresses the requirements of your Organisation, but 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 is not lightened by virtue of the Covid-19 pandemic, but rather it places Organisations in a unique environment that necessitates Employers 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 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 is the increased use of video conferencing necessitated by the Covid-19 mitigation measures. 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

- 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 utilised 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 to advise Employees to avoid sharing of company 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.

Disclaimer - The information in this section is provided to assist Employers on the implementation of the government restrictions and must be read in the context of information provided by the Data Protection Commission website and should not be interpreted as a legal definition of any of the information provided. The information is changing constantly, and any information provided is correct of April 13, 2020 and is per information on the Data Protection Commission website as of that date.

For further information or advice, please contact the experienced HR and Employment Law team in Adare Human Resource Management – 01 561 3594 or ipihrhelpdesk@adarehrm.ie