Medtronic

the wheel Stronger Charities. Stronger Communities. adare human resource management

Data Protection & Remote Working – Ensuring Legislative Compliance

In late February, the Data Protection Commission (DPC) published its Annual Report for 2020, highlighting an increase of 9% in the number of cases it handled in 2020, up from 9,337 in 2019 to 10,151 in 2020. A total of 4,660 complaints were received under GDPR, with "Access request" and "Fair processing" making up over half of these. The report also stated that *"cases concerning employment law disputes continue to be heavily represented in the range of complaints received".* However, it also stated *"it's becoming an increasing feature of the complaints received by the office that issues are being raised with the DPC that, in truth, have little or nothing to do with data protection".*

The report also highlighted that of the 6,673 breaches of GDPR, just one related to the charity sector and 16 to the voluntary sector. But it is still reminding employers and employees what they need be mindful of when remote working.

Data protection considerations for remote working

The seismic shift to remote working across all sectors including the Community, Charity and Not-for-Profit sector presented new challenges for employers in terms of data protection. Ensuring employees were aware of their responsibilities to protect sensitive information, update security software and regularly change passwords became all the more important. Even what might seem like simple things like the minimal use of paper is crucially important, especially if the information contained relates to sensitive personal medical information, such as counselling notes. Data protection still applies to paper files as well as electronic files.

People should continue to be careful when using USBs, phones and ensure laptops are not misplaced or left unattended as well as making sure devices are always locked.

Only trusted networks or cloud servers that comply with the organisation's rules and procedures should be used. Many organisations have also asked employees to ensure "listening" devices such as Amazon Echo should not be in the same room if work-related calls are being conducted.

Use of video conferencing

One of the biggest changes stemming from remote working is the increased use of video conferencing. We have all become very accustomed to Zoom and Teams for meetings, one-to-one meetings and counselling sessions. The DPC set out some useful tips on the safe use of video conferencing to help ensure adequate data protection.

- Employees should use service providers as agreed or contracted by the employer who, equally, ensure they are comfortable with the privacy and security features of the platform.
- Only use work accounts, email addresses, phone numbers, etc, for work-related video conferencing, to avoid the unnecessary collection of their personal contact or social media details.
- Clear and updated policies and guidelines should be in place on the use of video conferencing. These should outline responsibilities and rules and steps that should be taken to minimise data protection risks.

- 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.
- Employees need 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.

Use of CCTV within organisations

One specific question that is being asked is around the use of CCTV, particularly in relation to monitoring employees. Under Data Protection legislation CCTV cameras may be used in the workplace and would normally be in place for the protection of staff, service users and the premises. However, it is necessary that those people whose images are captured on camera are informed about the identity of the purpose of capturing the data. Therefore, it is necessary that signs confirming use of CCTV cameras are placed in prominent positions in the workplace and are easily legible.

It is considered very intrusive to use CCTV to monitor the performance of employees and would need to be justified by reference to special circumstances. The DPC has previously noted that that a balance must be struck between the privacy of the employee and the interests of the employer.

If CCTV cameras are to be used in the unlikely situation of disciplinary action, the employer must have a policy in that regard so that employees are aware that footage captured maybe used for this purpose and a rationale for this type of use must be provided. Also, if CCTV footage is being used in a disciplinary process as evidence, the employee should be given the opportunity to view the evidence in advance of a disciplinary hearing to allow them to prepare a defence.

While organisations remain in the remote working space it is of critical importance that data protection considerations are communicated to staff so that everyone is aware of the requirements to maintain compliance with legislation.