LK SHIELDS
YOUR LEGAL COUNSEL

DATA PROTECTION, PRIVACY AND SECURITY

Back to Basics – DPC Decision in Move Ireland

by

Back to Basics – DPC Decision in Move Ireland

21st December 2021 | by

A recent DPC decision in respect of a data breach at the charity MOVE Ireland reinforces the importance of getting the basics right: **Plan – Do – Check – Act.**

Introduction

On 20 August 2021 the Data Protection Commission (DPC) issued several corrective actions in its decision against the charity MOVE Ireland. This included the imposition of a fine, a reprimand and the imposition of various orders to bring MOVE into compliance with Data Protection Law. While at a glance the decision may not appear to be relevant to most organisations, a review of the DPC's findings reveals that this decision has many important lessons for any organisation working with personal data. The decision highlights through extreme examples the importance of properly planning and implementing a data protection strategy for any kind of processing an organisation undertakes. We would advocate an approach of Plan – Do – Check – Act.

Background

MOVE (Men Overcoming Violence) Ireland is a charity working in the area of domestic violence. It holds weekly group counselling sessions for men during which they are encouraged to take responsibility for their violence and to ultimately change their attitudes and behaviours. MOVE employs 35 facilitators who lead weekly sessions across Ireland. Facilitators were required to record the sessions on SD cards, which were later uploaded to OneDrive folders. On 3 February 2020 MOVE informed the DPC that a personal data breach had occurred after it discovered that 18 of the 44 SD cards were missing.

Plan

The decision highlighted that MOVE had failed to undertake some of the basic planning that is required before processing any kind of personal data. Under the GDPR, organisations are expected to maintain the integrity and confidentially of personal data in a manner that 'ensures appropriate security'. This means that organisations must assess the security required against the risk to the rights and freedoms of a data subject. Recital 76 of the GDPR helpfully states that data controllers should have regard to the nature, scope, context and purpose of the processing when carrying out this assessment.

In this decision the DPC noted that the nature of the processing was extremely serious – it included images and sounds relating to extremely sensitive personal data. This had to be weighed against the purpose of the processing, which in this context was to allow MOVE to manage and deliver its 'Choices Programme'. However, the purpose of the recordings were to 'assess the skills of the facilitators in their role and to provide appropriate feedback, training and supervision to them'. The DPC in reviewing this balance noted the GDPR's data minimisation principle in that data collected for a particular purpose, in this case training, should be adequate, relevant and limited to what is necessary for that purpose. The DPC felt that MOVE had not considered the risks involved if a facilitator lost an SD card.

It was, in particular, noted that there was a failure to consider alternative ways to assess the skills of facilitators and provide them with training. One example would be to have an experienced facilitator attend

the group sessions in person. This alternative seemed far more appropriate and avoided many of the risks associated with the high-risk activity of recording these sessions.

This decision illustrates the importance of considering whether a risk assessment is necessary before carrying out a processing activity. Under the GDPR a risk assessment is not necessary for every type of processing activity but a justification for deciding not to carry out an assessment can be just as important.

Your organisation might not be videoing highly sensitive counselling sessions, but a similar risk-based assessment should be carried out on many of your organisations processing activities to see if there is an alternative approach to achieving the same goal. Your assessment should consider compliance with all six data protection principles.

Do

Once you have planned out what processing activities are required and are confident you have chosen the least intrusive way to carry these risks out, you need to implement the appropriate security measures for the data you have collected.

The Data Controller has an obligation to store the data securely. The greater the risk to the rights and freedoms to an individual (as identified by a risk assessment) the greater the security measures that should be put in place. The DPC said that although some measures had been put in place, MOVE had failed to properly identify the risk that could stem from the mishandling of SD cards by facilitators.

The DPC noted that risks had been identified by MOVE, such as a transport risk in moving SD cards to its HQ, and MOVE had provided that the video files should be uploaded to OneDrive. However, many of the practices outlined by MOVE were considered inadequate. Foremost of these for most organisations was the approach of MOVE to audits and training. Both of these were implemented as a once-off occurrence as opposed to as an ongoing obligation. The audit of the risks and standards within MOVE in particular was framed as a once-off exercise in GDPR implementation, this audit was carried out in 2018. The DPC stressed that such an audit should have been carried out on a more regular basis.

Check

One of the most important factors in a sound data protection programme is the need for ongoing checks. The DPC stressed in its decision that there were no reviews of the effectiveness of particular procedures. MOVE identified to the DPC two security measures that it had implemented: firstly, that it provided training to facilitators in handling the video recordings; and secondly, that it had policies, procedures and oversight in place. However, the DPC found that there was no oversight provided by MOVE to confirm that the procedures required were being properly implemented or even effective. For example, no oversight was provided to confirm that the SD cards had indeed been wiped by a facilitator after the upload. The DPC suggested that regular audits of the effectiveness of the security measures should be carried out.

Act

The final stage of an effective data protection strategy is to implement the findings of the regular review that you carry out. The MOVE decision highlights the ongoing nature of the GDPR's obligations. The DPC in its decision said that "creating policies and procedures is essential to implementing an appropriate level of security. However, policies and procedures alone are not sufficient to mitigate risk.".

DPC held that MOVE had failed to identify and mitigate future risks, and noted in particular that, no regular testing was carried out of the processes that were in place.

Some measures suggested by the DPC as examples included:

- Having two or more members of staff to oversee and sign off that recordings had been deleted.
- Having a documented security policy and regular audits to confirm these were being carried out.
- Providing adequate and regular training to all staff in MOVE's policies and procedures, rather than only providing training when someone is hired.

Remember

This article considered certain essential principles of a data protection strategy.

- A data breach does not mean that someone else must have accessed the data and can instead result from a much broader set of circumstances.
- Know the six data protection principles and consider them constantly whenever you are dealing with personal data.
- Consider the risk involved in processing and whether a risk assessment is necessary, if you decide that no such assessment is necessary keep a record of your reasoning.
- Obligations cannot be fulfilled by a once-off implementation but should be reviewed on an ongoing basis.

If you would like to learn more about anything in this note, or how these issues may apply to your organisation, please contact Aideen Burke or your usual contact in our Data Privacy team.

About the Authors