Article 25 of the General Data Protection Regulations(Art.25 GPDR) prescribes that the data controller integrates data protection into the system by design and default (Bygrave, 2017). The controller is required to implement technical and administrative controls to ensure, by default, data processing is limited to what is necessary given the purpose for which the data is initially collected(privacy by design)and be limited to those who need to access the data(privacy by default)

In the case of An Garda Síochána (AGS), it was not mentioned if the data contained in the DVD media, which was part of the evidence file, was encrypted (potential violation of data pricy). The regulation requires the controller to pseudonymise and minimise data (Facts, 2018).

Furthermore, Article 35(Art. 35 GPDR) requires the controller to conduct a risk assessment with a Data Privacy Impact Assessment (DPIA) (Mantelero, 2019). A thorough risk assessment impacts analysis influences how administrative and technical controls are utilised to reduce the risk. The controller needed to investigate the probabilities of accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data stored in the evidence file.

Although punitive action was taken against the investigating officer believed to have never returned the file, the loss of the file exposed vulnerability in the system. Object access and tracking control need to be implemented in the system. Officers need to provided with access to evidence objects in a controlled manner where the custodian of the evidence objects and the subjects use an electronic system that tracks the duration the officers need access to evidence objects. The system should alert the controller should evidence items not be returned at the required time. Thus, implementing a tracking system will enable the controller to report data loss accurately and timeously to the regulator. Employees should be trained to take the responsibility to safeguard sensitive and confidential information.

References

Bygrave, L. A. (2017) ‘Data Protection by Design and by Default : Deciphering the EU’s Legislative Requirements’, *Oslo Law Review*, 1(02), pp. 105–120. doi: 10.18261/issn.2387-3299-2017-02-03.

Facts, Q. (2018) ‘GDPR Physical Security and Privacy Safeguards’.

Mantelero, A. (2019) ‘Comment to Articles 35 and 36’, *GDPR Commentary*.