In the matter of the General Data Protection Regulation

DPC Case Reference: IN-20-7-1

In the matter of MOVE Ireland

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

20 August 2021

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**'the Decision'**) is a decision made by the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**). I make this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act. A member of the inquiry team of the DPC (**'the Case Officer'**) provided MOVE (Men Overcoming Violence) Ireland (**'MOVE'**) with a Draft Inquiry Issues Paper in order to make submissions on it.

1.2 MOVE was provided with the Draft Decision ('**the Draft Decision'**) on this Inquiry on 20 July 2021 to give it the final opportunity to make submissions. This Decision is being provided to MOVE pursuant to section 116(1)(a) of the 2018 Act in order to give MOVE notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

1.3 This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (**'the GDPR'**) arising from the infringements which have been identified herein. In this regard, MOVE is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on MOVE in accordance with section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2 Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of section 109(5)(e) or section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

ii. Data Controller

2.3 In commencing the Inquiry, the DPC considered that MOVE may be the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of the personal data breach. In this regard, MOVE confirmed that it was the controller, both in its notification of the personal data breach to the DPC on 3 February 2020[1] and in the content of the *MOVE Ireland Data Protection Policy 2018*, which was provided to the DPC in MOVE's submissions of 18 September 2020.[2]

iii. Legal Basis for the Decision

2.4 Section 111 of the 2018 Act requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry, as well as submissions that MOVE has furnished to me, and any other materials which I consider to be relevant in the course of the preparation of this Decision.

2.5 The Inquiry Issues Paper was finalised on 22 December 2020. MOVE made submissions on the Draft Inquiry Issues Paper on 30 November 2020. On 20 July 2021 I issued the Draft Decision to MOVE. MOVE made submissions on the Draft Decision on 10 August 2021. A full schedule of all documentation considered by me for the purpose of the preparation of this Decision is appended hereto.

2.6 Having considered the information obtained in the Inquiry, I am satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. I had also regard to the submissions that MOVE decided to make in respect of the Draft Decision on 10 August 2021 before proceeding to make this Decision under section 111 of the 2018 Act.

3. Factual Background

3.1 MOVE is a company limited by guarantee and a registered charity[3], which works in the area of domestic violence, with a primary aim of supporting the safety and wellbeing of women and their children who are experiencing, or have experienced violence/abuse in an intimate relationship. MOVE does this by facilitating men (**'participants'**) in weekly group

[1] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 1.
[2] Appendix D.3.b – Data Protection Policy 2018, page 2.
[3] MOVE Ireland is a company limited by guarantee, CRO No. 254239, and a registered charity, Revenue: CHY 11382 / Registered Charity Number (RCN): 20031077. This information is available in MOVE IRELAND CLG, *Annual Report 2019,* available at https://www.moveireland.ie/move-ireland-reports/ (last) access on 2 June 2021, page 1.

sessions with a facilitator encouraging them to take responsibility for their violence and changing their attitude and behaviour.

3.2 MOVE also has responsibility for the management and delivery of the Choices Programme, which is funded by the Department of Justice. In 2019, the Choices Programme saw the participation of over 200 men.[4]

3.3 MOVE has four area co-ordinators and thirty-five facilitators nationwide[5] who were required to undertake the recording of the group sessions (**'recording of group sessions'**) on SD memory cards (**'SD Cards'**) and who took responsibility for the storage of the SD Cards. Those facilitators were responsible for saving the recordings onto laptops and uploading them onto the One Drive.[6] MOVE outlined that recordings of group sessions were introduced in September 2017.[7] MOVE also clarified that it operates eleven group programmes across Ireland and each programme has four SD Cards, for a total of forty-four SD Cards.[8]

3.4 MOVE notified the DPC of the personal data breach on 3 February 2020. The data breach notification concerned the loss of SD Cards that may have contained recording of group sessions of MOVE's Choices programme where participants discuss their behaviour and attitudes with regard to domestic violence with a facilitator.[9]

3.5 MOVE stated that it became aware that some SD Cards were missing in the Sligo area on 16 December 2019.[10] After becoming aware of this, MOVE reported that it conducted an internal audit to locate all SD Cards across the organisation. The audit determined that eighteen out of a total of forty-four SD Cards were missing, and that three of the eleven areas had their full quota of cards.[11]

3.6 MOVE reported that the eighteen missing SD Cards have not been located.[12] Whilst the recording of group sessions focused on the delivery of sessions by the facilitators, some of the participants may have been seen and heard in the recordings[13]; furthermore the personal data on the SD Cards included participants' disclosure of behaviours, feelings and attitudes towards current or ex partners, other family members and friends, who may have been named by the participants[14]. MOVE submitted that 80 to 120 men may have been affected by this personal data breach.[15]

[4] MOVE IRELAND CLG, *Annual Report 2019, op. cit.,* page 14.
[5] In addition, MOVE is overseen by a Board of Trustees (6) and has a member of staff (in addition to the areas co-coordinators and facilitators) a Chief Executive Officer, a National Administrator/ Board Secretary, a Finance Officer, a Part-time Development Officer, a Partner Support Worker for Dublin, cfr. MOVE IRELAND CLG, *Annual Report, op. cit.,* pages 3-5.
[6] Appendix D.3.f – Role of Facilitator, page 7.
[7] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 3.
[8] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 2.
[9] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 1 and 2.
[10] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 2.
[11] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 2.
[12] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 2-3.
[13] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 2.
[14] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 2.
[15] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 2.

3.7 The DPC issued an Inquiry Commencement Letter ('**the Commencement Letter'**) by email and registered post to MOVE on 12 August 2020 notifying the organisation that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act. The letter contained details of the personal data breach notified to the DPC which would be the subject of the Inquiry and contained eleven questions seeking further information from MOVE.

3.8 The decision to commence the Inquiry was taken having regard to the circumstances of personal data breach notified by MOVE. The Commencement Letter informed MOVE that the Inquiry would examine whether or not MOVE discharged its obligations in connection with the subject matter of that personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by MOVE in that context. In this regard, the scope of the Inquiry was expressly stated to include the steps taken by MOVE to comply with the principle of integrity and confidentiality pursuant to Article 5(1)(f) of the GDPR and the technical and organisational measures taken by MOVE to ensure security of processing pursuant to Article 32(1) of the GDPR.

3.9 The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The relevant facts ascertained during the personal data breach notification and handling process were set out in the Commencement Letter. The facts, as established during the course of the Inquiry, are set out below in this Decision.

3.10 MOVE provided submissions in response to the Commencement Letter on 18 September 2020. In its submissions, MOVE outlined the technical and organisational measures which MOVE had in place to meet the requirements of the GDPR. The submissions outlined policies and procedures in relation to data protection governance, including requirements for the facilitators it employs.

3.11 The submissions also outlined the steps that MOVE has taken since the personal data breach in order to comply with the GDPR including details of the security measures which will be put in place allowing MOVE to cease using SD Cards in the future. The submissions appended a number of documents, which are considered throughout this Decision.

3.12 On 23 September 2020, the Case Officer requested additional documentation related to the MOVE Ireland Property, Equipment and Assets Policy. MOVE provided the policy by return on the same day.

3.13 On 9 November 2020, further submissions were sought from MOVE specifically with regard to the role of its facilitators. MOVE provided its submissions on the matter on 11 November 2020.

3.14 Having received MOVE's submissions, the DPC proceeded to prepare a Draft Inquiry Issues Paper to document the relevant facts established and the issues that fell for consideration by me as decision maker for the purpose making a decision under section 111 of the 2018

Act in respect of this Inquiry. The Case Officer furnished MOVE with the Draft Inquiry Issues Paper on 17 November 2020 and invited MOVE's submissions on any inaccuracies and/or incompleteness in the facts.

3.15 MOVE provided comments on the Draft Inquiry Issues Paper on 30 November 2020. The comments included some textual amendments and supplemental information relating to the facts as set out in the Draft Inquiry Issues Paper. Those comments were analysed and the DPC prepared the Inquiry Issues Paper.

3.16 On 22 December 2020, the DPC finalised the Inquiry Issues Paper. On 20 July 2021 I provided the Draft Decision to MOVE. MOVE was afforded the opportunity to make submissions on the proposed infringements that were provisionally identified in the Draft Decision and the corrective powers that I proposed to exercise. On 10 August 2021 MOVE made submissions on the Draft Decision. I have had full regard to those submissions and I have reached conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

4. Scope of the Inquiry and the Application of the GDPR

4.1 The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not MOVE discharged its obligations in connection with the subject matter of the personal data breach and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by MOVE in that context.

4.2 In this regard, the Commencement Letter specified that the Inquiry would focus on MOVE's organisational and technical measures in place to ensure security of the personal data. In particular, the Commencement Letter expressly stated that the scope of the Inquiry would include Articles 5(1)(f) and 32(1) of the GDPR. The Commencement Letter stated that the Inquiry would focus on the areas of Security of Personal Data, Data Protection Governance, Training and Awareness, and Records Management.

4.3 Article 2(1) of the GDPR defines the Regulation's scope as follows:

> *This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

4.4 Recital 15 of the GDPR provides guidance for interpreting the material scope of the GDPR:

> *In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are*

contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

4.5 Article 4(1) of the GDPR defines 'personal data':

'*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

4.6 *Ryneš* judgement[16] provides further clarification of what personal data is in the context of video (images and sounds) recording. In this case, the Court of Justice of the European Union ('the **CJEU**') examined the operation of a CCTV system, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitored a public space. The CJEU held that:

"the image of a person recorded by a camera constitutes personal data […] inasmuch as it makes it possible to identify the person concerned."[17]

4.7 The European Data Protection Board ('the **EDPB**') in its Guidelines on processing of personal data through video device further explains that collection of image or audio-visual information allows people to be:

"identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons´ presence and behaviour in the given space." [18]

4.8 Article 4(6) of the GDPR defines 'filing system':

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

4.9 Images and sounds of both the participants and the facilitators, therefore, fall within the definition of personal data as it is clear they could either be directly identified on the basis of these data (such as, for example, through their images) or easily identifiable in combination with other personal information (such as, for example, through any additional

[16] Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů,* judgement of 11 December 2014 (ECLI:EU:C:2014:2428).
[17] Case C-212/13, *František Ryneš, op. cit,* para 22.
[18] EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2019 on processing of personal data through video devices*, Version 2.0, Adopted on 29 January 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (last) access on 3 June 2021, para 7.

personal information that participants may have disclosed with reference to their behaviours, feelings and attitudes). Furthermore, to the extent participants disclosed personal information in relation to their family members during the recordings of group sessions, it is likely the SD Cards contain the personal data of third parties additionally.

4.10 The sounds and images recorded onto SD cards form part of a *'filing system'* because SD Cards consist of physical storage devices for electronic data that is organised into one or more partitions that contain a file system, to allow access to the contents. By default, SD Cards use the File Allocation Table (FAT) family of file systems (FAT16, FAT32, exFAT).[19]

4.11 The session facilitators used camcorders to record the sessions. These devices used automated means to transfer the video sound and image onto each SD Card, while the manual removal of the populated SD Cards to insert them into laptops involved the processing of personal data that resided within a filing system on those cards.

4.12 In this case, the SD Cards contained the personal data of MOVE's participants and facilitators. Therefore, the personal data processed by MOVE on the SD Cards fall within the scope of the GDPR.

5. MOVE's submissions in relation to the Draft Decision

5.1 The Draft Decision was provided to MOVE on 20 July 2021, and MOVE was requested to furnish any submissions it wished to make to the DPC by 11 August 2021. MOVE furnished its submissions in respect of the Draft Decision on 10 August 2021 ('**Submissions in relation to the Draft Decision'**). MOVE stated that its submissions were in respect of the proposed administrative fine, which MOVE considered excessive[20]. [redacted]

5.2 As clarified above, although the decision to commence the Inquiry was taken having regard to the circumstances of the personal data breach notified by MOVE, the Inquiry and this Decision do not assess the compliance with the obligation pursuant to Article 33 of the GDPR. Rather it is the case that this Inquiry and this Decision examine MOVE's compliance with the principle of integrity and confidentiality pursuant to Article 5(1)(f) of the GDPR and the technical and organisational measures taken by MOVE to ensure security of processing pursuant to Article 32(1) of the GDPR.

5.3 For the avoidance of doubt, as further assessed in Part 7, this Decision examines the appropriateness of the technical and organisational measures in place at the time of the

[19] See the definition of Secure Digital Card (SD Card) available at techopedia, https://www.techopedia.com/definition/2808/secure-digital-card-sd-card (last) access 3 June 2021.
[20] Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 1.

personal data breach in the context of processing of recordings of group sessions on SD Cards. The personal data breach, as further explained below, was ultimately caused by various failures of the technical and organisational measures.

5.4 However, I have considered MOVE's submissions relating to the nature of the personal data breach and the consideration of the notification of this personal data breach to the DPC, and I set out my views in respect of these matters below. Part 8.C.i. deals with my further consideration and analysis of MOVE's submissions regarding its view that the administrative fine proposed in the Draft Decision was excessive.

5.5 In the Submissions in relation to the Draft Decision, MOVE appears to define the personal data breach it notified to the DPC on 3 February 2020 as a potential breach and it further clarified that "*It is not known if there was in fact a breach of data protection*"[21].

5.6 Article 4(12) of the GDPR defines 'personal data breach':

> *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

5.7 The Article 29 Working Party, in its Guidelines on Personal data breach notification under Regulation 2016/679 ('**Personal Data Breach Notification Guidelines'**) further clarifies what constitutes a personal data breach and with specific reference to the loss of personal data it explains:

> *"In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession"*[22]

5.8 Considering the definition of "personal data breach" pursuant to Article 4(12) GDPR, it is evident that the notified personal data breach involving the loss of the SD Cards containing recordings of group sessions constitutes a personal data breach. As further clarified by the Personal Data Breach Notification Guidelines, MOVE, as controller, had lost control of the personal data, which were recorded on the SD Cards. Having regard to the circumstances of this personal data breach, the DPC decided to commence an Inquiry to determine whether or not MOVE was in compliance with Article 5(1)(f) and Article 32(1) of the GDPR. The fact that the lost SD Cards may or may not contain actual personal data is a further demonstration of the fact that MOVE did not apply its own data protection policies and procedures properly *at the time* of the personal data breach, as detailed in Part 7.iii. Nonetheless, as assessed in Part 8.C.i, I have considered the lack of evidence regarding the extent of the personal data contained on the lost SD Cards when determining whether to

[21] Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 1.

[22] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guideline on Personal data breach notification under Regulation 2016/679*, 18/EN WP250rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, , endorsed by the EDPB on 25 May 2018, available at https://ec.europa.eu/newsroom/article29/items/612052 (last access) 13 August 2021, page 7.

impose a fine and the amount of that fine. Therefore, I am of the view that the personal data breach notified by MOVE on 3 February 2020 was a personal data breach.

5.9 In its Submissions in relation to the Draft Decision, it seems that MOVE also alleged that it was not obliged to notify the personal data breach to the DPC, and its notification should be considered as a mitigating factor in the determination of the amount of the administrative fine in order also to incentive other controllers to notify similar personal data breaches.[23]

5.10 Article 33(1) of the GDPR imposes the specific obligation for controllers to notify personal data breaches to the supervisory authority:

> *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."*

5.11 Where a controller fails to notify a personal data breach to the supervisory authority, this may lead to a supervisory authority exercising its powers pursuant to Article 58 GDPR, including but not limited to the imposition of an administrative fine in accordance with Article 83 GDPR. This is further clarified in the Personal Data Breach Notification Guidelines:

> "*If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures.*"[24]

5.12 Furthermore, as detailed in Part 8.C.i, compliance with the obligation to notify a personal data breach to the supervisory authority cannot be considered a mitigating factor in the determination of the amount of the administrative fine. Therefore, I am of the view that MOVE correctly, and in line with its obligations as controller, notified the personal data

[23] MOVE stated: "*In an abundance of caution and to ensure we adhered to our responsibilities in every way possible we took it upon ourselves to notify the Data Protection Commission of the potential for a breach of GDPR"* (page 1); "*We would submit that it is a mitigating factor that we approached the supervisory authority in respect of what we saw as a risk of a breach of GDPR but where in fact there was no evidence of an actual breach. Again, we would submit that it would negatively impact on organisations, and be contrary to public policy, to impose a fine on our organisation in these circumstances and it may in fact deter other organisations in similar circumstances from coming forward to you"* (page 2), cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 1-2.

[24] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guideline on Personal data breach notification, op. cit,* page 9-10.

breach; however, this compliance with a legal requirement cannot be considered a mitigating factor.

6. Issue for Determination

6.1 The Inquiry Issues Paper identified the following questions and issues that arise for determination:

a) An assessment of the risks of varying likelihood and severity for the rights and freedoms of natural persons associated with MOVE's processing of personal data on the SD cards, having regard to MOVE's own assessment of these risks;

b) Whether the measures implemented by MOVE were appropriate to ensure the ongoing confidentiality of the processing of personal data on the SD cards, having regard to the level of governance implemented over the cards and their contents, the level of training and awareness provided to staff, and the lack of encryption of the files on the SD cards;

c) The extent to which the consideration of question (a) above and the appropriateness of the measures to ensure ongoing confidentiality must be assessed in light of the fact there was no confirmed evidence in this Inquiry of an actual unauthorised disclosure of the personal data to a third party particularly given that MOVE is not certain that the missing cards have actual recordings on them;

d) Whether the measures implemented by MOVE were appropriate to ensure the ongoing availability and resilience of MOVE's processing systems and services, having regard to the circumstances in which MOVE's audit found that eighteen out of the forty-four SD cards were missing; and

e) Whether the measures implemented by MOVE were appropriate in light of any obligation that it may have been under to implement a process for regularly testing, assessing and evaluating the effectiveness of its technical and organisational measures in respect of the security of the SD cards.

6.2 Therefore, having considered the Commencement Letter, the Inquiry Issues Paper and the other relevant materials, I find that it falls for me to consider in this Decision whether MOVE has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data of participants and facilitators processed in connection with recordings of group sessions on SD Cards.

7. Issue: Articles 5(1)(f) and 32(1) of the GDPR

7.1 Article 5(1)(f) of the GDPR provides for the principle of integrity and confidentiality. It requires that personal data shall be:

> *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

7.2 Article 32(1) of the GDPR elaborates on the principle of integrity and confidentiality in Article 5(1)(f) by setting out criteria for assessing what constitutes *'appropriate security'* and *'appropriate technical or organisational measures'*:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *a) the pseudonymisation and encryption of personal data;*
>
> *b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

7.3 Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data. There is an obligation to consider "*the state of the art*" with regard to measures available. This term "*state of the art*" is not defined within the GDPR. By dictionary definition, it is defined as "*using the latest techniques or equipment*".[25]

7.4 The term "*state of the art*" has been considered by the EDPB in its Guidelines on Article 25 of the GDPR. These Guidelines state that:

> *18. The concept of "state of the art" is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the "state of the art" is made*

[25] Concise Oxford Dictionary, (8th ed., BCA & Oxford University Press, 1991).

not only in Article 32, for security measures, but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.

19. In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, ***to take account of the current progress in technology t****hat is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape.*

20. The "state of the art" is a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed continuously in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25.

21. The "state of the art" criterion does not only apply to technological measures, but also to organisational ones. Lack of appropriate organisational measures can lower or even completely undermine the effectiveness of a chosen technology. Examples of organisational measures can be adoption of internal policies; up-to date training on technology, security and data protection; and IT security governance and management policies.[26]

7.5 In those Guidelines, the EDPB included two footnote references to further consideration of the "*state of the art*" in the context of Article 32 of the GDPR. Both footnotes refer to guidelines prepared by TeleTrusT - IT Security Association Germany in cooperation with the European Union Agency for Network and Information Security. Those TeleTrusT guidelines state:

…the "state of the art" can be described as the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives.

In short it can be said that the "state of the art" describes a subject's best performance available on the market to achieve an object.[27]

[26] EUROPEAN DATA PROTECTION BOARD, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, version 2.0, adopted on 20 October 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (last) access on 3 June 2021.

[27] TELETRUST IN COOPERATION WITH ENISA, *IT Security Act (Germany) and EU General Data Protection Regulations: Guideline "State of the art". Technical and organisational measures*, 2020, available at https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-10_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf (last) access 3 June 2021, page 11.

i. Assessing Risk

7.6 Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement an appropriate level of security. The level of security must be appropriate to the risk presented to the rights and freedoms of natural persons, and must have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. Therefore, the first step is to assess the risk presented to the rights and freedoms of data subjects by the processing of personal data, and then to assess the appropriateness of the security measures implemented (as detailed in the following Parts 7.ii and 7.iii).

7.7 Recital 76 of the GDPR provides guidance as to how risk should be evaluated:

> *The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*

7.8 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others* judgement[28] provides further guidance on the risk assessment. In this case, the CJEU declared the Data Retention Directive[29] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The CJEU held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to:

> *(i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.*[30]

7.9 Considering the CJEU approach, it appears that risk is assessed objectively by reference to (i) the likelihood of the risk to the rights and freedoms of natural persons, and (ii) the severity of that risk. Hence, the risk assessment must consider, first, the likelihood of the risk to the rights and freedom of participants and facilitators posed by the processing of recordings of group sessions; and second, the severity of that risk in respect of the rights

[28] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

[29] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[30] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd, op. cit,* para 66.

and freedoms of the data subjects. These objective assessments must be made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data. Only in light of the risk assessment is possible to analyse the appropriateness of the security measures implemented (as detailed in the following Parts 7.ii and 7.iii).

7.10 Thus, it is necessary first to analyse the nature, scope, context and purposes of the processing. The nature of MOVE's processing of personal data is serious as it involves the recording of personal data (images and sounds) relating to participants and facilitators. The seriousness of the processing is related to the high quantity and the sensitive nature of the personal data processed.

7.11 The quantity of personal data processed by MOVE in the recording of group sessions is significant; at the time of the personal data breach, MOVE was using forty-four SD Cards to record group sessions in various locations across the country. MOVE indicated that some of the SD Cards may contain three to four sessions recorded on them and that each session would have involved four to nine participants.[31] Each session would have also involved at least one facilitator. MOVE estimated that 80 to 120 men may have been affected by the notified personal data breach alone. [32]

7.12 The personal data processed by MOVE is at the higher end of the scale of sensitivity. MOVE's recordings concern weekly group sessions that encourage participants to take responsibility for their violence and to change their attitude and behaviour. Therefore, the personal data processed likely includes references to personal information related to sex life (pursuant to Article 9). It also likely includes personal data relating to criminal convictions and offences or related to security measures (pursuant to Article 10) for some participants. These personal data, by its very nature, are particularly sensitive with regard to the fundamental rights and freedoms of data subjects. In addition, the recordings likely contain references made by the participants during the sessions to other vulnerable people. Thus, the sensitive nature of personal data processed by MOVE increases the severity of the risks, as illustrated in Recital 75 of the GDPR.

7.13 The scope and the context of processing of the participants' and facilitators' personal data in the recordings of group sessions is linked to MOVE's responsibility for the management and delivery of the Choices Programme, a key feature of which includes conducting group sessions. MOVE also confirmed that it does not share the recordings of the group sessions with the group participants or any parties outside of the organisation.[33]

[31] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 2.
[32] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 2.
[33] MOVE clarifies in its Digital Recording Protocol "*There are no other circumstances within which sessions will be digitally recorded. Digital recordings will not be used in external settings or to provide evidence in criminal justice proceedings as no consent has been obtained for this purpose. The recordings are a training and development tool only […] No session recording or part thereof will be made available to any other services (internal or external) under any circumstances*.", cfr. Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 5.

7.14 The purposes of MOVE's processing of personal data relates to MOVE's functions of managing and delivering the Choices Programme. MOVE clarified that the purpose of recording group sessions is to allow MOVE to fully assess the skills of the facilitators in their role and to provide appropriate feedback, training and supervision to them in that role.[34] As specified in MOVE's *Digital Recording Protocol*, recordings are a standard training tool in delivering this type of service.[35] I note that MOVE submitted that participants consented to the recordings of group sessions.[36] However, given the requirement that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and in light of the purposes relied on by MOVE, it may be questioned whether there are alternative ways to assess the skills of the facilitators in their role and to provide appropriate feedback, training and supervision without recording group sessions. For example, a practice of having experienced facilitators attend the group sessions of other facilitators and provide feedback after the group session could reduce the risk to the rights and freedoms of participants and facilitators. The recording of the group sessions is aiming only at supervising and improving the skills of the facilitators, despite the fact that it increases the risk to rights and freedoms of participants. However, these latter matters are beyond the scope of this Decision which focus on Articles 5(1)(f) and 32(1) compliance.

7.15 I find that there was a high risk, both in likelihood and severity, to the rights and freedoms of natural persons, from MOVE's processing of recordings of group sessions containing personal data of participants and facilitators (and of the people to whom participants may have referred in the recorded sessions). The high severity of the risk to the rights and freedoms of natural persons occurred due to the quantity and the sensitive nature of the processing undertaken by MOVE in the context in which it was undertaken. The provision of the service provided by MOVE is intrinsically linked to the rights and freedoms of facilitators, participants and other persons with whom they interact, and a loss or an unauthorised disclosure of their personal data has significant capacity to infringe those rights and freedoms. The high likelihood of the risk related to the potential for loss and unauthorised disclosure of personal data was heightened by MOVE's use of SD Cards for temporary storage. Responsibility for the security of these SD Cards rested with, amongst others, thirty-five facilitators, who were expected to follow MOVE's policies and procedures. Each facilitator had responsibility for recording the group sessions on the SD Cards and then uploading these recordings to One Drive. Each facilitator also had the responsibility for erasing the recordings from each SD Card after each upload. This created a risk that facilitators could fail to appropriately handle the recordings and the SD Cards, including by failing to appropriately erase the recordings or by losing the SD Cards. In all the circumstances, the likelihood of the risk to the rights and freedoms of the data subjects was high.

[34] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 1.
[35] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 5.
[36] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 1.

ii. Security Measures Implemented by MOVE

7.16 MOVE's submissions outlined the technical and organisational measures that it had in place at the time of personal data breach. The measures relevant to MOVE's processing of personal data on the SD Cards can be categorised as:

a) Policies, Procedures, and Oversight,
b) Training and Awareness.

7.17 In implementing appropriate security measures, the obligation falls on the controller to first consider the risk presented to the rights and freedoms of natural persons by the relevant processing of personal data. In this case, the processing concerns MOVE's recordings of group sessions as assessed above. Having assessed this risk, the controller must then implement measures that are appropriate in light of the risk. MOVE stated that in preparation for the GDPR it undertook an audit of Data Protection Measures in May and June 2018. This audit identified the transportation of the SD Cards[37] to the Dublin or Ennis Offices as a risk[38] and MOVE put measures in place to alleviate this risk by enabling facilitators to upload the recordings to local area One Drives. Based on this consideration, MOVE adopted specific technical and organisational measures (as outlined below). However, in the first instance, it does not appear that MOVE fully assessed the risks related to its processing of recordings of groups sessions, including the risk that facilitators could fail to appropriately handle the recordings and the SD Cards, for example, by failing to appropriately erase the recordings or by losing the SD Cards. Furthermore, it does not appear that MOVE performed any risk assessment with reference to its new approach of storing on SD Cards and local uploading directly by facilitators. If MOVE had conducted an appropriate risk assessment on its processing of recordings of group sessions, it might have considered various alternative options to mitigate the risks and decided to not use the SD Cards for temporary storage. MOVE intends to replace the SD Cards with alternative measures for storing the recordings and this illustrates that there were additional measures that MOVE could have implemented regarding the risk at the time of the personal data breach.[39]

[37] MOVE stated: *"Prior to this audit SD cards were being collected by coordinators from facilitators and taken to the Dublin and Ennis Offices for uploading and deletion of files and were then transported back to facilitators.",* cfr. Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.

[38] MOVE stated "*As part of the implementation of GDPR, Move Ireland conducted an audit of client files between May 3rd and June 7th in order to improve the procedures regarding the collection and storage of personal data. Recording of sessions and in particular the physical transfer of these files was identified as a risk*", cfr. Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.

[39] MOVE ultimately reported "*Please note that MOVE Ireland have moved away from using SD cards for the recording of sessions. Group work sessions have been suspended since the outbreak of covid-19. When groupwork resumes all recordings will be undertaken using a webcam and uploaded on to the one drive as before.*" cfr., Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 2.

(a) Policies, Procedures and Oversight

7.18 MOVE outlined that it had introduced a range of policies and procedures in relation to data protection as part of the implementation of GDPR. In particular, MOVE conducted an audit between May and June 2018 in order to improve the procedures regarding the collection and storage of personal data. It stated that Microsoft One Drive was implemented on the laptops used in each local area to mitigate the risk of transporting SD Cards and to allow for the uploading of files locally, therefore negating the need for transporting the SD Cards.[40]

7.19 MOVE outlined that all of its laptops were encrypted to ensure that recordings would be safely stored on the laptop prior to uploading to Microsoft One Drive.[41]

7.20 MOVE's facilitators were required to adhere to data protection policies and were required to sign these on an annual basis from September 2018,[42] indicating that they had read and understood data protection implications of the video recording and storage. MOVE clarified in particular that:

> *"Instructions were given to the facilitators that the video recordings must be focused on the facilitators and that as far as possible, clients should not be in view of the camera. This was reinforced at local demonstration sessions."* [43]

and that

> *"Instructions were also given to facilitators to delete recordings from the SD card once the file was uploaded on to the one drive. These files in turn were deleted from the one drive after 4 months."*[44]

7.21 MOVE also provided the following policies with its submissions:

- Data Protection Policy 2018 (Appendix D.3b)
- Retention and Destruction Policy (Appendix D.3c)
- Record Keeping and File Management Procedures (Appendix D.3d)
- Role of Facilitator (Appendix D.3f)

7.22 The *Retention and Destruction Policy* sets out that video recordings are retained for a period of four months. The *Data Protection Policy* states that

> *"any media holding video files will be stored in a locked filing cabinet."*[45]

[40] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.
[41] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.
[42] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.
[43] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.
[44] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 2.
[45] Appendix D.3.b – Data Protection Policy 2018, page 4.

Both the *Retention and Destruction Policy* and the *Record Keeping and File Management Procedures* contain an affirmation statement to be signed by facilitators that indicates that they have read and agree with the policies. Both documents contain the following wording:

> *"I understand that failure to keep accurate records or the inappropriate sharing of information could amount to professional misconduct and / or a breach of data protection legislation.*
>
> *"I accept that inappropriate sharing of information or failing to keep accurate records could lead to disciplinary procedures."*[46]

7.23 The *Role of Facilitator* document provided by MOVE describes how recordings were to be handled by facilitators following a group session:

> *"Whilst the process may vary slightly depending on local circumstances the following process should be followed.*
>
> 1. *Session is recorded using the camcorder and SD card*
> 2. *At the end of the group session, facilitator saves the recording on to the laptop. This should not take more than 20 minutes.*
> 3. *Once recording has been successfully saved on to the laptop, the recording on SD card is deleted and placed back in the camcorder.*
> 4. *If wi-fi access is strong, video is immediately uploaded on to the one drive. If wi-fi is either weak or non-existent, a facilitator takes responsibility for taking laptop home and uploading file on to the one drive."*[47]

7.24 With reference to oversight of MOVE's policies and procedures, the *Data Protection Policy* states that:

> *"All files should be stored in a safe and secure designated place. In the absence of central base, all staff will be expected to ensure files are stored in safe and secured place. When a room containing files is left unattended it should be locked. In each location where the files are held a system will operate where a line manager will oversee the security system.*
>
> *These managers will be responsible for ensuring that there is a security system in operation where all files are held in secure cabinets, which are locked at the end of the day and that if staff have a file in their offices, the file will be locked away when that person leaves work for the day."*[48]

[46] Appendix D.3.c – Retention and Destruction Policy, page 6. Appendix D.3.d – Record Keeping and File Management Procedures, page 5.
[47] Appendix D.3.f – Role of Facilitator, page 7.
[48] Appendix D.3.b. – Data Protection Policy, page 4.

7.25 As reported above, MOVE also stated that it provided "*local demonstrations*" to facilitators on how to focus the video recording on the facilitator and how to record and delete the sessions.[49] However, MOVE has not provided any documented record of such activities.

7.26 MOVE also confirmed that:

> *"The recordings were saved to the laptops and then uploaded on to the area one drive.* ***Line managers would have monitored the uploading*** *of recordings to ensure that this was taking place."*[50] (emphasis added)

7.27 It appears from the above description, therefore, that MOVE should have been in a position to identify which facilitators last uploaded files and to cross check that information with those facilitators holding SD Cards. However, MOVE outlined in its submissions that if there were recordings on the missing SD Cards, some videos may have contained images of facilitators and participants[51]. The audit undertaken by MOVE in May and June 2018 was carried out as part of the implementation of GDPR, rather than being an ongoing organisational measure in place *at the time* when the personal data breach occurred. In addition, MOVE was not able to provide a record of processing in relation to the data population and erasure of the content of the missing SD Cards.[52] Furthermore, it appears from the above description that MOVE should also have been in a position to oversee facilitators' compliance with MOVE's policies and procedures. However, MOVE was not able to provide any records regarding the "*local demonstrations*" and, as reported above, MOVE stated that *at the time* of the personal data breach such oversight "*would have*" been in place.

7.28 I note that after the personal data breach and during the conduct of the Inquiry, MOVE expressed its intention to stop using the SD Cards in the context of its recording of group sessions.[53]

(b) Training and Awareness

7.29 The facilitators are employed by MOVE on one year contracts running from August to July. MOVE outlined that data protection training was provided to all staff at its November 2018 Annual General Meeting.[54] The training was a once off session and there is no record of

[49] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1 and 2
[50] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, pages 3-4.
[51] Appendix D.4.b – MOVE's Response to Issues Paper, dated 30 November 2020, page 2.
[52] In the personal data notification form submitted by MOVE on 3 February 2020, in response to the question "*Please outline why you have not secured/retrieved the data*", MOVE replied "*We have not been able to find the SD cards. We do not know if the lost SD cards have data on them as the recordings would have been wiped once they were uploaded on to the one drive and deleted after 6 months. All the remaining SD cards are securely stored and data has been deleted from all cards*", Appendix D.1.a – Breach Notification, dated 3 February 2020, page 3.
[53] MOVE ultimately reported "*Please note that MOVE Ireland have moved away from using SD cards for the recording of sessions. Group work sessions have been suspended since the outbreak of covid-19. When groupwork resumes all recordings will be undertaken using a webcam and uploaded on to the one drive as before.*" cfr., Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 2.
[54] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.

training for facilitators retained since that date. The controller was also unable to provide training records for the facilitators who had been in possession of the SD Cards that were subsequently lost.

7.30 With reference to training and awareness, the *Data Protection Policy* states that*:*

> *"Not all staff members will be expected to be experts in Data Protection legislation. However, MOVE Ireland is committed to ensuring that its staff have sufficient awareness of the legislation to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Designated Data Protection Lead is informed, in order that appropriate corrective action is taken."*

and it continues:

> *"If any member of staff is uncertain as to the meaning of any of the provisions and procedures herein, the staff member should consult with their manager or the Designated Data Protection Lead to seek clarification."*[55]

7.31 The *Retention and Destruction Policy* further specifies:

> *"The Designated Data Protection Lead will arrange for every employee to receive a copy of this Policy and each such employee shall sign a statement that affirms that he or she has received a copy of this Policy, has read and understands it, and has agreed to comply with it. There will be a training for staff as part of the roll-out of the Policy."*[56]

7.32 MOVE's duty regarding training and awareness is not limited to once off training modules. In light of the sensitivity of the personal data handled by facilitators, I consider that an appropriate level of security must include ongoing data protection and awareness training to facilitators. Therefore, the training methods demonstrated by MOVE did not meet standard required by the GDPR. Moreover, it does not appear that there were any measures in place to prevent facilitators even to use their own personal SD Cards .These risks are borne out by the fact that MOVE was unable to confirm what personal data may have been on the SD Cards which went missing. In this case, it was pivotal to have effective measures in place to provide oversight of compliance with the policies and procedures, as well as an effective record/tracking and storage system of SD Cards.

iii. The Appropriate Level of Security

7.33 Having regard to the high risk to the rights and freedoms of data subjects, in terms of both likelihood and severity, presented by MOVE's processing of participants' and facilitators' personal data processed in connection with recordings of the group sessions on SD Cards, with the acknowledgement that special category data may be processed, an appropriate

[55] Appendix D.3.b. – Data Protection Policy, page 2.
[56] Appendix D.3.c. – Retention and Destruction Policy, page 1.

level of security must include standard operating procedures setting out how that personal data is processed, retained and deleted. The policies provided by MOVE set out these considerations. However, an appropriate level of security must also include oversight by MOVE of the ongoing implementation of their policies and procedures and appropriate checks and balances to ensure that they are followed. I find that MOVE's policies were not adequate to ensure a level of security appropriate to the risk as there was insufficient oversight measures and checks and balances system in place to guarantee compliance by facilitators with MOVE's own policies and procedures. This lack of oversight measures and check and balances resulted in the failure of the policies and procedures.

7.34 Article 32(1)(d) of the GDPR specifies that appropriate technical and organisational measures may include **regular** processes for testing, assessing and evaluating the effectiveness of existing measures. Such testing, assessing and evaluating applies to both **technical and organisational measures**. Personal data breaches may cause significant harm to data subjects and, pursuant to Article 32(1)(d), controllers must take the initiative to test, assess, and evaluate their organisational and technical security measures.

7.35 An appropriate level of security includes **technical measures** that have, *inter alia*, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. It is apparent that the use of SD Cards as a transfer medium introduced a risk of losing unencrypted personal data. At the time of the personal data breach, it appears that the ability to encrypt SD Cards while recording on camcorders may not have been a feature that was readily available on commercial cameras. The process of using an unencrypted SD Card as a storage medium was inherently insecure. The intention of MOVE to alter the process to avoid using such SD Cards indicates that there was an alternative process available to be used at the time of the personal data breach.

7.36 An appropriate level of security includes **organisational measures** that enable MOVE to test, assess and evaluate the effectiveness of those measures. The audit of Data Protection Measures undertaken by MOVE in May and June 2018 identified that the transportation of the SD Cards was a risk and measures were put in place to alleviate this risk enabling recordings to be uploaded on to local area One Drives by facilitators. However, I find that MOVE failed to identify and mitigate further risks concerning facilitators' data collection and storage using SD Cards. For example, additional measures which ought to have been in place include a process for regularly testing, assessing and evaluating the effectiveness of MOVE's existing security measures; and the implementation of measures for recording the location of, and accountability for, the SD Cards containing personal data throughout its facilitator network.

7.37 An appropriate level of security includes **organisational measures** to ensure at least that there is:

- Documentation of the security policy of the controller and the procedures to be followed by staff;
- Adequate training of all staff in those policies and procedures;

- Checks and balances system in place as ordinary procedure where, for example, two or more members of staff have to oversee and sign-off that recordings have been deleted from the SD card;
- Oversight of ongoing implementation of those policies and procedures.

7.38 Creating policies and procedures is essential to implementing an appropriate level of security. However, policies and procedures alone are not sufficient to mitigate the risk to data subjects. Where staff handle sensitive personal data, the provision of appropriate training and awareness is even more important. Having considered that a controller must regularly assess and evaluate the effectiveness of measures in place, there must be an ongoing and verifiable oversight of how the staff members give effect to the controller's policies and procedures.

7.39 MOVE reflects the importance of training and awareness in its own policies and it provided one training session to staff in November 2018. Considering the high risk of the processing activities related to the recording of group sessions, I find that a once off session cannot be considered appropriate to the level of risk. MOVE stated that facilitators are employed on a one year contract (from August to July) and it did not provide any documentation that facilitators were given further training after November 2018 and before the personal data breach. For example, it might be possible that a change of the facilitators happened since November 2018 and new facilitators may or may not have data protection training appropriate for MOVE's processing. Furthermore, MOVE did not provide any documentation or records of refresher training for existing or renewed staff.

7.40 MOVE's facilitators are contractually obliged to follow the specific procedures; however, it appears that MOVE confirmed that there was a lack of oversight by line managers. Furthermore, notwithstanding its own policies and procedures, MOVE was not able to provide any record or tracking of the SD Cards, including in respect of the identity of the facilitator responsible for each SD Card and how many participants were recorded on each of the SD Cards. These issues ultimately led to the personal data breach and to MOVE's subsequent failure to locate eighteen of the missing SD Cards without any certainty as to whether personal data of participants and facilitators may be on those missing SD Cards.

7.41 Accordingly, I find that there were inadequate procedures to ensure that facilitators were adhering to the security policies, in that there was no guarantee that recordings retained on the SD Cards were deleted in line with the *Role of Facilitator* document. Moreover, there were inadequate procedures to control each instance of the upload of personal data from the SD Cards to facilitators' laptops and the subsequent deletion of the data from the SD Cards as set out in the *Role of Facilitator* document. It is not clear how line managers within MOVE could monitor each instance of the upload of personal data from the SD Cards to facilitators' laptops, given that MOVE has thirty-five facilitators and four area co-ordinators (line managers). Finally, I find that there was a failure to adequately track and log the location of the SD Cards.

iv. Findings

7.42 I find that MOVE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of recording of group sessions on SD Cards containing participants' and facilitators' personal data.

8. Corrective Powers

8.1 I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that MOVE has infringed Articles 5(1)(f) and 32(1) of the GDPR. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not those infringements merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

8.2 Recital 129 of the GDPR, which acts as an aid to the interpretation of Article 58, provides that *"… each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case …."* In the circumstances of the within Decision, and with particular reference to the findings arising therefrom, I find that the exercise of one or more corrective powers is both appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR.

8.3 Having carefully considered the infringements, I have decided to exercise corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringements in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2). In summary, the corrective powers that I have decided to exercise are:

a) Article 58(2)(b) – I have decided to issue a reprimand to MOVE in respect of its infringements of Articles 5(1)(f) and 32(1) of the GDPR;
b) Article 58(2)(d) – I have decided to order MOVE to bring its processing into compliance with Articles 5(1)(f) and 32(1) of the GDPR;
c) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR.

A. Reprimand

8.4 I issue MOVE with a reprimand in respect of its infringements of Articles 5(1)(f) and 32(1) of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to "*issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation*." In accordance with Recital 129 of the GDPR, in imposing a corrective power, I must ensure that it is "*…appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…".*

8.5 I consider that a reprimand is appropriate, necessary and proportionate in view of ensuring compliance with the infringed Articles as the reprimand, along with the other corrective measures, will act to formally recognise the serious nature of all of the infringements. Further, the reprimand emphasises the requirement for MOVE to take all relevant steps to ensure future compliance with Articles 5(1)(f) and 32(1) of the GDPR.

8.6 Recital 148 of the GDPR is provides:

> *"In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine."*

8.7 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. In this respect, I consider it appropriate, necessary and proportionate to impose a reprimand in addition to the order in Part 8.B and the administrative fine in Part 8.C of this Decision. The decision to impose a reprimand is based on the serious nature of the infringements of Articles 5(1)(f) and 32(1) of the GDPR. The objective of these Articles is to ensure that controllers and processors implement a level of security that is appropriate to the risk presented by their processing operations. MOVE's infringements of these Articles is serious in light of the sensitivity of personal data that it processes and in light of the inappropriate technical and organisational measures. I consider that the imposition of a reprimand is both appropriate, necessary and proportionate in light of the importance of ensuring compliance with Articles 5(1)(f) and 32(1) of the GDPR in the context of protecting the fundamental rights and freedoms of data subjects. I consider that it is appropriate, necessary and proportionate to recognise the seriousness of non-compliance of this nature with a reprimand in light of that objective of ensuring compliance with Articles 5(1)(f) and 32(1) of the GDPR.

8.8 Therefore, I consider that the formal recognition of the seriousness of the infringements of Articles 5(1)(f) and 32(1) of the GDPR by means of a reprimand is appropriate and necessary to ensure compliance with these Articles. A reprimand is proportionate in the

circumstances where it does not exceed what is required to ensure compliance with the GDPR, taking into account the seriousness nature of the infringements and the potential for harm to data subjects.

B. Order to Bring Processing into Compliance

8.9 In accordance with Article 58(2)(d) of the GDPR, I order MOVE to bring its processing operations regarding its recordings of group sessions into compliance with Articles 5(1)(f) and 32(1) of the GDPR. This order would require MOVE to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

8.10 In making this decision to impose this order, I have had regard to MOVE's intention to stop using the SD Cards in the context of the recordings of group sessions. However, I consider that this order is necessary to ensure that full effect is given to MOVE's obligation to implement appropriate technical and organisational measures in the context of its ongoing recordings of group sessions. In deciding that an order is appropriate to achieve this end, I have had particular regard to the sensitivity of personal data processed and the key role played by the facilitators as considered in this Decision. Therefore, I consider that additional technical and organisational measures are essential to protect the rights and freedoms of data subjects. MOVE must perform the necessary risk assessment to inform the measures that it must implement. However, as outlined above, those measures should include at least:

a) The encryption of the SD Cards subject to confirmation from MOVE of its intention to continue to use them in the context of the recordings of group sessions. If MOVE ceases its use of the SD Cards, it must implement an alternative appropriate technical and organisational measures to secure the recordings of group sessions;
b) Adequate data protection training for staff and measures to promote the awareness of staff with regard to data protection requirements relating to their roles and responsibilities and MOVE's policies and procedures;
c) Measures to implement a specific records management system with reference to the recordings of group sessions. This system should make provision for tracking the recordings, including but not limited to, their creation, storage, movement, retention and destruction.
d) Effective oversight measures and checks and balance system in place to guarantee compliance with MOVE policies and procedures by members of staff.

8.11 In the Draft Decision I invited MOVE to make specific submissions on the matter of the timeframe for bringing the processing operations into compliance with Articles 5(1)(f) and 32(1) of the GDPR with specific measures. MOVE submitted that it would provide a report to the DPC outlining the steps it has taken to bring its processing into compliance by **30 September 2021**. I, therefore, order MOVE to bring its processing operations regarding its recordings of group sessions into compliance with Articles 5(1)(f) and 32(1) of the GDPR by

30 September 2021. MOVE must also submit a report to the DPC outlining the steps it has taken in respect of each of these measures on or before **30 September 2021**.

8.12 It must be noted that implementing these measures does not relieve MOVE of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by its processing of personal data in the context of the of recordings of group sessions.

C. Administrative Fine

8.13 In addition to the corrective powers under Article 58(2)(b) & (d), I have also decided that MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR warrant the imposition of an administrative fine. The reason for that decision, and the method for calculating that fine are set out below.

8.14 In the Submissions in relation to the Draft Decision, MOVE submitted that the proposed administrative fine was excessive, addressing each of the criteria pursuant to Article 83(2) of the GDPR. I have considered those submissions, and I set out my consideration and analysis of MOVE's submissions with reference to each of the criteria pursuant to Article 83(2) of the GDPR in the below Part.

i. Whether the Infringements Warrant an Administrative Fine

8.15 Article 58(2)(i) permits the DPC to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in section 115 of the 2018 Act, which permits the DPC to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2).

8.16 Article 83(1), in turn, identifies that the administration of fines *"shall in each individual case be effective, proportionate and dissuasive"*. In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) GDPR, which provide that:

> *"Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

8.17 The decision as to whether to impose an administrative fine (and if so, the amount of the fine) is a cumulative decision which is taken having had regard to of the factors as set out in Article 83(2)(a) to (k). Therefore, I will now proceed to consider each of these criteria in turn in respect of MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR:

a) <u>the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;</u>

8.18 The nature of MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR comprises a failure to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing operations concerning the recording of group sessions on SD Cards. The objective of Articles 5(1)(f) and 32(1) is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data

breaches occur. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to data subjects.

8.19 The gravity of the infringements of Articles 5(1)(f) and 32(1) of the GDPR is serious in circumstances where the infringements resulted in the personal data breach. I have had regard to the lack of certainty concerning the extent of the personal data on the SD Cards and the fact that the eighteen lost SD Cards have not been located. I acknowledge that there is no evidence of actual unauthorised third party access to personal on the lost SD Cards. There is also a lack of certainty regarding the number of data subjects affected by the personal data breach; 80 to 120 men may have been affected by the personal data breach [57] and, at least one, facilitator per each recorded session. There is also potential for third party data subjects who may have been mentioned in the sessions to have been affected. Nonetheless, assessed objectively, I consider that the potential level of damage suffered by the data subjects had the potential to be high when considered in light of the purpose of MOVE's processing and the sensitivity of the personal data processed by MOVE. As outlined above, the purpose of the processing of personal data is to improve MOVE's functions of managing and delivering the Choices Programme, and assessing the skills of the facilitators in their role.[58] In this context, in each recording session participants may have disclosed to the facilitator personal data, including special categories, and personal information related to their family members. While there is a lack of certainty around whether there has been unauthorised access to the personal data on the lost SD Cards, and, if so, the extent of that access, I consider that the breach of security leading to the loss of the personal data is serious in these circumstances. In light of that personal data breach, which flowed from MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR, I assess those infringements to be on the high end of the scale of gravity.

8.20 Regarding the duration of the infringements of Articles 5(1)(f) and 32(1) of the GDPR, the personal data breach occurred on 16 December 2019. MOVE introduced the recordings of group sessions in September 2017.[59] MOVE also stated that it conducted an audit as part of the implementation of GDPR between 3 May and 7 June 2018[60] and, on the basis of this audit, MOVE decided to begin uploading each recording session on SD Cards locally into One Drive by facilitators. I find that the infringements of Articles 5(1)(f) and 32(1) of the GDPR commenced at the enactment of the GDPR in May 2018 (25 May 2018). MOVE did not fully assess the risks related to its processing of recordings of groups sessions, including the risk that facilitators could fail to appropriately handle the recordings and the SD Cards, and then failed to implement appropriate measures in light of this processing. Notwithstanding MOVE's decision to upload the recording of group sessions locally, MOVE failed in implementing and overseeing its own policies and procedures to ensure a level of security appropriate to the risk. This Decision considers the security measures that MOVE

[57] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 2.
[58] Appendix D.1.c – MOVE's response to DPC, dated 19 February 2020, page 1.
[59] Appendix D.1.a – Breach Notification, dated 3 February 2020, page 3.
[60] Appendix D.3.a – MOVE's Response to Commencement Letter, dated 18 September 2020, page 1.

implemented at the time of the personal data breach. This Decision does not make findings in relation to the level of security that MOVE currently implements and it is acknowledged that MOVE implemented a number of additional measures following the discovery of the personal data breach, including by conducting an internal audit to locate all SD Cards across the organisation. Therefore, for the purposes of this Decision, the duration of the infringements must be assessed as commencing at 25 May 2018 and ending on the date of the personal data breach on 16 December 2019. Therefore, the duration is one year and about seven months in length.

8.21 In the Submissions in relation to the Draft Decision, MOVE disagreed with the nature of the personal data breach and submitted that "*It is not known if there was in fact a breach of data protection and our notification to you was out of an abundance of caution*"[61]. As further assessed in Part 5, this Decision examines the infringements of Articles 5(1)(f) and 32(1) of the GDPR. From this standpoint, the analysis in this Decision is related to the technical and organisational measures in place at the time of the personal data breach to ensure a level of security appropriate to the risk in respect of its processing operations concerning the recording of group sessions on SD Cards. As detailed above, the failure to implement the appropriate technical and organisational measures led ultimately to the personal data breach. I have had full regard to the fact that there is no evidence of actual unauthorised third party access to personal data on the lost SD Cards when deciding whether to impose a fine and when deciding on the amount of the fine. However, in light of MOVE's most recent submission that it is not known if there was a breach or not, it is important to emphasise that the definition of "personal data breach" in Article 4(12) of the GDPR (as fully detailed in Part 5) includes destruction, loss, alteration, unauthorised disclosure of, or access to personal data. As outlined above, I consider that the breach of security leading to the loss of the personal data is serious in these circumstances.

b) <u>the intentional or negligent character of the infringement;</u>

8.22 The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 ('the **Administrative Fines Guidelines**') provide that:

> *"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."*[62]

8.23 I do not consider that there was "*intent*" on the part of MOVE in respect of its infringements of Articles 5(1)(f) and 32(1) in the sense that there was "*knowledge*" or "*wilfulness*'" on the

[61] Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 1.
[62] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679,* 17/EN, WP 253, adopted on 3 October 2017, endorsed by the EDPB on 25 May 2018, available at https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en (last) access on 29 June 2021, page 11.

their part in respect of their failure to implement an appropriate level of security. However, I am satisfied that MOVE was negligent and breached the duty of care required of it by failing to implement and oversee its policies and procedures related to the processing of recordings group session.

8.24 In the Submissions in relation to the Draft Decision, MOVE submitted that it was neither intentional nor negligent, since procedures were in place.[63] As recalled above, Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data. MOVE's implementation of its policies were not adequate to ensure a level of security appropriate to the risk as there were insufficient oversight measures and checks and balances in place to guarantee compliance by facilitators with MOVE's own policies and procedures. In these circumstances, I consider accordingly that there was a negligent character to MOVE's infringements of Articles 5(1)(f) and 32(1) of the GDPR.

c) <u>Any action taken by the controller or processor to mitigate the damage suffered by data subjects;</u>

8.25 The infringements of Articles 5(1)(f) and 32(1) of the GDPR resulted in a personal data breach and the personal data, namely those potentially saved onto the eighteen SD Cards, was never retrieved. Due to the lack of appropriate organisational measures, MOVE was also unable to identify the number of affected data subjects (participants and facilitators) and, consequently to adopt any measures to mitigate the damage suffered by the data subjects. MOVE was unsuccessful in locating the eighteen missing SD Cards. In those circumstances, I find that MOVE did not take any action to mitigate the damage suffered by data subjects. However, MOVE's failure to take action to mitigate the damage suffered by the data subjects was, in fact, caused by its same failure to implement appropriate organisational measures that forms the basis for the findings of infringements of Articles 5(1)(f) and 32(1) in this Decision. Its failure to track the SD Cards, including in respect of the identity of the facilitator responsible for each SD Card and how many participants were recorded on each of the SD Cards, not only contributed towards the personal data breach, but also subsequently prevented MOVE from taking steps to mitigate potential damage suffered by the data subjects. In the particular circumstances, the infringement also resulted in a lack of evidence regarding the extent of the personal data contained on the lost SD Cards, including whether personal data had been deleted before the loss of the SD Cards. In circumstances where MOVE's infringements of Article 5(1)(f) and 32(1) also prevented it from taking action to mitigate the potential damage suffered by the data subjects, I do not consider this absence of action can be considered an aggravating factor in respect of those same underlying infringements.

[63] MOVE stated with reference to Article 83(2)(b): "*Procedures were in place to avoid an infringement of the data protection regulations and no breach has in fact been proven and therefore we submit that the breach is purely one of potential and therefore neither intentional nor negligent*", cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 1.

d) <u>the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;</u>

8.26 As outlined above, MOVE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures regarding its recording of group sessions on SD Cards.

8.27 In the Submissions in relation to the Draft Decision, MOVE submitted that measures were in place to prevent any potential breach of data protection.[64] I have had full regard to those measures in Part 7 of this Decision. This Decision assesses whether MOVE complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data of participants and facilitators processed in connection with recording of the group sessions on SD Cards. As detailed in Part 7, MOVE failed in this regard.

8.28 I consider that MOVE holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(f) and 32(1) against MOVE, this factor cannot be considered aggravating in respect of those infringements.

e) <u>any relevant previous infringements by the controller or processor;</u>

8.29 There are no relevant previous infringements by MOVE.

f) <u>the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;</u>

8.30 In the Submissions in relation to the Draft Decision, MOVE underlined that it cooperated proactively in respect of the Inquiry.[65] I accept MOVE's submission that it cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its breach notifications and during the Inquiry, it illustrated the steps that it had taken and was in the course of taking to remedy the infringements and the possible adverse effects. These steps included, amongst others, the intention to replace its use of the SD Cards in the context of its recording of group sessions.

g) <u>the categories of personal data affected by the infringement;</u>

8.31 I consider that the categories of personal data affected by the infringements of Articles 5(1)(f) and 32(1) of the GDPR included sensitive personal data. As outlined in Parts 4 and 7 of this Decision, the personal data concerned images and sounds of participants and

[64] MOVE stated with reference to Article 83(2)(d) of the GDPR: "*Measures were in place to prevent any potential breach of data protection*." cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 2.
[65] MOVE stated with reference to Article 83(2)(f) of the GDPR: "*We co-operated in every way and indeed were pro-active in following up with the Data Protection Commission in respect of the investigation*", cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 2.

facilitators. In particular, in discussing their behaviours, feelings, and attitudes, participants may have also disclosed special categories of personal data pursuant to Articles 9 and 10 of the GDPR and personal data related to potential vulnerable third parties, namely their family members. In the Submissions in relation to the Draft Decision, MOVE stated that "*it is not known if there was in fact a breach*".[66] While it is not known whether there was unauthorised access to this personal data, the inadequate security measures implemented related to this sensitive personal data. I find that the sensitivity of these categories of personal data aggravates the infringements of Articles 5(1)(f) and 32(1) in circumstances where the personal data lost have not been retrieved.

h) <u>the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;</u>

8.32 The Inquiry was conducted to examine whether or not MOVE has discharged its obligations in connection with the subject matter of the personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by MOVE in that context.

8.33 In the Submissions in relation to the Draft Decision, MOVE stated that "*It was our organisation that made the potential for an infringement known to the supervisory authority".*[67] As further clarified in Part 5, controllers are obliged to notify personal data breaches in certain circumstances and MOVE's notification of the personal data breach indirectly contributed to the infringements of Articles 5(1)(f) and 32(1) of the GDPR becoming known to the DPC.

8.34 The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> *"The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor."*[68]

8.35 MOVE's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 5(1)(f) and 32(1) of the GDPR.

[66] MOVE reported this comment with reference to Article 83(2)(g) of the GDPR, cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 2.
[67] MOVE reported this comment with reference to Article 83(2)(h) of the GDPR, cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 2.
[68] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines, op. cit.,* page 15.

i) <u>Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;</u>

8.36 The corrective powers have not previously been ordered against MOVE with regard to the subject-matter of this Decision.

j) <u>adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;</u>

8.37 Not applicable.

k) <u>any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement;</u>

8.38 In the Submissions in relation to the Draft Decision, MOVE stated:

> "*We would submit that it is a mitigating factor that we approached the supervisory authority in respect of what we saw as a risk of a breach of GDPR but where in fact there was no evidence of an actual breach. Again, we would submit that it would negatively impact on organisations, and be contrary to public policy, to impose a fine on our organisation in these circumstances and it may in fact deter other organisations in similar circumstances from coming forward to you*".[69]

8.39 In Part 5, I have addressed the nature of what constitutes a personal data breach and the obligation for controllers to notify a personal data breach. As also assessed above with reference the criteria pursuant to Article 83(2)(h) of the GDPR, MOVE's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 5(1)(f) and 32(1) of the GDPR. I wish to further underline that the failure to notify a personal data breach pursuant to Article 33(1) GDPR may lead a supervisory authority to exercise its powers pursuant to Article 58 GDPR in respect of such a failure to notify, including but not limited to the imposition of an administrative fine in accordance with Article 83 GDPR.

8.40 I consider, therefore, that the matters considered under Article 83(2)(a) – (k) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case. In doing so, I have also considered MOVE's Submissions in relation to the Draft Decision.

8.41 Given the specific circumstances of the case at hand, and having particular regard to the matters discussed under Article 83(2)(a) – (j) cumulatively, I consider it appropriate to

[69] MOVE reported this comment with reference to Article 83(2)(k) of the GDPR, cfr. Appendix - D.6.a - MOVE submissions on the Draft Decision, dated 10 August 2021, page 2.

impose an administrative fine in addition to the reprimand and order imposed at Parts 8.A and 8.B of this Decision.

8.42 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. The Administrative Fines Guidelines provide that:

> *"The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both)."*[70]

8.43 I find that an administrative fine is necessary in order to effectively pursue the objective of re-establishing compliance with the Articles 5(1)(f) and 32(1) of the GDPR and in providing an effective, proportionate and dissuasive response in the particular circumstances of this case. In order to re-establish compliance with Articles 5(1)(f) and 32(1), it is necessary to dissuade non-compliance.

8.44 In reaching this decision to impose an administrative fine, I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. In particular, I have had regard to the reprimand and order made in Parts 8.A and 8.B of this Decision. The order has significant value in re-establishing compliance because it obliges MOVE to take certain specified steps in implementing technical and organisational measures. The reprimand, on the other hand, is of significant value in dissuading future non-compliance. This formal recognition of the seriousness of MOVE's infringements is likely to contribute to ensuring an appropriate level of security going forward.

8.45 However, having considered the nature of the infringements of Articles 5(1)(f) and 32(1), I find that those corrective powers alone are not effective and proportionate in re-establishing compliance and in dissuading future non-compliance. Articles 5(1)(f) and 32(1) place a continuous obligation on controllers and processors to regularly test, assess and evaluate the effectiveness of the technical and organisational measures that it has implemented. Furthermore, the appropriate level of security must be continually re-assessed in light of the dynamic risk presented by MOVE's processing and the state of the art.

8.46 Therefore, compliance with the order in Part 8.B of this Decision alone cannot ensure perpetual compliance with Articles 5(1)(f)and 32(1) going forward, as the risk changes and as new measures emerge in respect of these processing operations. Furthermore, I do not consider that the reprimand alone is an effective and proportionate response to the

[70] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the application and setting of administrative fines, op. cit.,* page 6.

infringements in light of the need to re-establish compliance and to dissuade non-compliance.

8.47 In coming to the conclusion that an administrative fine is necessary and appropriate, I have particular regard to the gravity and the duration of the infringements (as assessed in accordance with Article 83(2)(a) above). Those infringements pose a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur. I consider that an administrative fine is necessary in light of the potential for damage to data subjects by such non-compliance. This is because an administrative fine is necessary to effectively protect those rights by re-establishing compliance and to deterring future non-compliance. I consider that an administrative fine is necessary in order to effectively protect those rights, despite the lack of certainty as to whether or not there was unauthorised access to the lost SD Cards in respect of the personal data breach.

8.48 Having decided that the infringements identified warrant the imposition of an administrative fine in the circumstances of this case, I must next proceed to decide on the amount of the administrative fine.

8.49 The findings of infringements of Articles 5(1)(f) and 32(1) relate to processing operations regarding MOVE's recording of group sessions on SD Cards. Article 32(1) elaborates on the requirement for appropriate security in Article 5(1)(f). In the circumstances, the infringements of Articles 5(1)(f) and 32(1) arise from the same failure of MOVE to implement an appropriate level of security. In those circumstances of this specific case, it is appropriate to calculate and apply a single administrative fine. Therefore, the fine will be calculated by reference to the infringement of Article 5(1)(f) only.

ii. The Applicable Range for the Administrative Fine

8.50 Having decided that the infringement of Article 5(1)(f) warrants the imposition of an administrative fine in the circumstances of this case, I must next proceed to decide on the amount of that fine. First, it is necessary to consider the appropriate cap for the fine as a matter of law. The cap determines the permitted range for the fine, from a range of zero to the cap. However, the cap is not a starting point for a fine. After identifying the permitted range, it is necessary to calculate the fine on that permitted range.

8.51 Article 83(5) of the GDPR provides that infringements of the obligations of controllers pursuant to, amongst others, Article 5 shall:

> *"…in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher…"*

8.52 The turnover of MOVE in 2019 was €686,421 as reported in MOVE's financial statements for 2019 available from the Company Registration Office's public repository. As regards the maximum amount for the fine that may be imposed in this case, the relevant cap for any fine in respect of an infringement of Article 5(1)(f) is the higher of €20,000,000 or 4% of the annual turnover of the preceding financial year. Therefore, I am satisfied that the cap for MOVE's infringement is €20,000,000. This figure is not a starting point, but rather the cap on the permitted range as provided for in Article 83(5) of the GDPR.

iii. Calculating Administrative Fine

8.53 In the absence of specific EU-level guidelines on the calculation of fines, I am not bound to apply any particular methodology[71]. In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the fine. Therefore, in calculating the fine I will identify the amount of the administrative fine to be imposed on MOVE on a general basis (as in the judgments cited in the footnotes above) and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

8.54 In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. This is compounded by the fact that future infringements need to be deterred. In this regard, I consider that a fine cannot be dissuasive if it will not be of any financial significance.

8.55 The Draft Decision set out a proposed range for the administrative fine and the factors to be considered, and the methodology to be used when calculating the fine, in order to provide MOVE with the opportunity comment in accordance with fair procedures. In its Submissions in relation to the Draft Decision, MOVE submitted various comments as outlined in the above paragraphs and in Part 5. MOVE submitted that the proposed administrative fine was excessive. For the reasons set out above, I do not accept these submissions. However, I accept MOVE's submission on their cooperation within the Inquiry.

8.56 As set above, the permitted range for the infringement of Article 5(1)(f) of the GDPR is up to €20,000,000 as provided for in Article 83(5) of the GDPR. In locating the administrative fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard

[71] See by analogy Case T 332/09, *Electrabel v Commission,* judgement of 12 December 2012 (ECLI:EU:T:2012:672), para 228; Case T-704/14, *Marine Harvest ASA v Commission*, judgement of 26 October 2017 (ECLI:EU:T:2017:753), para 450.

to the aggravating factors, specifically the negligent character of the infringement as assessed in accordance with Article 83(2)(b) above and the sensitivity of the categories of personal data affected in accordance with Article 83(2)(g). I have also had regard to the mitigating factors which I consider warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(e), and 83(2)(f) of the GDPR mitigating. Therefore, having regard to all of these factors, I consider that the administrative fine of **€1,500** is appropriate in the circumstances of this case.

8.57 I consider that the above administrative fine meets the requirements of effectiveness, proportionality and dissuasiveness of the administrative fine. In order for any fine to be effective, it must reflect the circumstances of the individual case. The circumstances of this infringement concerns the failure to implement an appropriate level of security in the context of recording of group sessions on SD Cards, which ultimately led to a personal data breach consisting of a loss of eighteen SD Cards. Those SD Cards have not been located and may contain sensitive personal data of participants and facilitators. I consider that these circumstances require a significant fine in order for it to be effective. In order for a fine to be dissuasive, it must dissuade the controller from repeating the conduct concerned. I am satisfied that the administrative fine would be dissuasive to MOVE. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any administrative fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the administrative fine does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringement on the data subject rights enshrined in the GDPR. Accordingly, I am satisfied that the administrative fine would be effective, proportionate and dissuasive, taking into account all of the circumstances of the case.

9. Right of Appeal

9.1 This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, MOVE has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is received by it. Furthermore, as this Decision includes a decision to impose an administrative fine, pursuant to section 142 of the 2018 Act, MOVE also has the right to appeal against the decision to impose an administrative fine within 28 days from the date on which notice of the Decision is given to it.

_____

Helen Dixon
Commissioner for Data Protection

Appendix: Schedule of Materials Considered for the Purposes of this Decision

D.1.a Breach Notification, dated 3 February 2020

D.1.b DPC's queries related to the breach notification to MOVE, dated 17 February 2020

D.1.c MOVE's response to DPC, dated 19 February 2020

D.1.d Email MOVE's query to DPC, dated 7 July 2020

D.1.e Email DPC's response to MOVE, dated 10 July 2020

D.1.f Email MOVE to DPC, dated 13 July 2020

D.2.a Commencement Letter, dated 12 August 2020

D.2.b MOVE's acknowledgement, dated 20 August 2020

D.2.c Reminder to MOVE, dated 14 September 2020

D.2.d MOVE's update, dated 14 September 2020

D.3.a MOVE's Response to Commencement Letter, dated 18 September 2020

D.3.b Data Protection Policy 2018

D.3.c Retention and Destruction Policy

D.3.d Record Keeping and File Management Procedures

D.3.e Facilitator Contract 2019-2020

D.3.f Role of Facilitator

D.3.g Property, Equipment and Assets Policy

D.3.h Queries and response re facilitators, 9 and 11 November 2020

D.4.a Draft Issues Paper, issued on 17 November 2020

D.4.b MOVE's Response to Issues Paper, dated 30 November 2020

D.5.a Inquiry Issues Paper, dated 22 December 2020

D.6.a MOVE submissions on the Draft Decision, dated 10 August 2021