An Coimisiún um Chosaint Sonraí
Data Protection Commission

Decision of the Data Protection Commission under Section 111 of the Data Protection Act 2018 on foot of the

Own-Volition Inquiry under Section 110 of the Data Protection Act, 2018

regarding

Tusla Child and Family Agency

Inquiry Reference: IN-19-12-8

Commission Decision-Maker:

Helen Dixon (Commissioner for Data Protection), sole member of the Commission

Date of Decision: 21st May 2020

Contents

1. Purpose of this Document 3
2. Background 3
3. The processing operation subject to this Decision 5
4. Legal regime pertaining to the Inquiry and Decision 6
5. Materials considered 6
6. Data Controller 7
7. Personal Data 7
8. Analysis and findings 7
   A. Security of Processing 7
      i. Assessing Risk 8
      ii. Security measures implemented by Tusla 11
      iii. The appropriate level of Security 12
      iv. Finding 13
   B. Data Breach Notification 14
      i. Analysis 14
      ii. Finding 16
9. Corrective Powers 16
   A. Reprimands 16
   B. Order to Tusla to bring its processing into compliance with Article 32(1) of the GDPR 16
   C. Administrative Fine 17
      i. Decision to impose an Administrative Fine 18
      ii. Calculating the Administrative Fine 24
10. Right of Appeal 26

1. Purpose of this Document

1.1 This document ("**the Decision**") is the decision of 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 separate own volition inquiry (**"the Inquiry"**) conducted by an Authorised Officer of the DPC (**"the DPC Investigator")**. The DPC Investigator who conducted the Inquiry provided Tusla Child and Family Agency ("**Tusla**") with the Draft Inquiry Report and the Final Inquiry Report. The Decision is being provided to Tusla pursuant to Sections 116(1)(a) of the 2018 Act in order to give Tusla notice of the Decision and the reasons for it, and the corrective powers that I have decided to exercise.

1.2 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 by the Decision Maker. Tusla is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on Tusla in accordance with Section 133 of the 2018 Act.

2. Background

2.1 On 15th March 2019, a social worker for Tusla wrote a safeguarding letter to the [redacted] The purpose of this letter was to inform [redacted] and to advise her of safeguarding procedures to ensure ongoing safety. However, the letter contained the names of [redacted] (**"the data subjects"**) who made the allegations and details of the allegations made. [redacted] subsequently shared a photograph of the safeguarding letter on [redacted]

2.2 On 12th April 2019, Tusla became aware that there may have been a personal data breach when [redacted] Tusla about the letter. On 31st October 2019, the local Tusla office referred the matter to Tusla's data protection unit. On 4th November 2019, Tusla notified the DPC of the personal data breach via the DPC's personal data breach web form (Breach Notification BN-19-11-81). On 12th November 2019, Tusla wrote to [redacted] providing information concerning the breach. Tusla wrote to the [redacted], who was not aware of the breach, inviting him to meet to discuss his case. [redacted] and Tulsa indicated in submissions to the DPC that it would issue a letter notifying him of the breach [redacted]

2.3 In response to the breach, Tusla contacted [redacted] requesting a meeting in order to retrieve the safeguarding letter and to request that the [redacted] Tusla has been unable to confirm that the letter has been retrieved and the [redacted] Tusla also issued a formal memo to

social work staff about considerations necessary when sharing information and appropriate governance regarding allegations of abuse.

2.4 On 11th December 2019, the DPC Investigator wrote to Tusla to notify it of the commencement of an own-volition inquiry pursuant to Section 110 of the 2018 Act regarding the personal data breach notified to the DPC. The letter informed Tusla that the Inquiry would examine whether or not Tusla had discharged its obligations in connection with the subject matter of the breach and would determine whether or not any provision(s) of the GDPR and/or the 2018 Act had been contravened by Tusla. The scope of the Inquiry was stated to include an examination of Tusla's compliance with Articles 5(1), 32(1) and 33 of the GDPR.

2.5 On 24th January 2020, the DPC Investigator issued the Draft Inquiry Report to Tusla. It set out the DPC Investigator's view on the data protection issues examined and on whether infringements of the GDPR or the 2018 Act had occurred. Tusla was invited to make submissions on the content of the Draft Inquiry Report. The DPC Investigator informed Tusla that he would consider any such submissions before proceeding to finalise the Inquiry Report.

2.6 On 21st February 2020, Tusla sent a submission document (**"the first submission"**) on the Draft Inquiry Report to the DPC Investigator. The DPC Investigator analysed the contents of the submissions and modified the report to correct two inaccuracies concerning the date of the Commencement Letter and the incorrect letter that was appended to the draft Inquiry Report.

2.7 On 24th February 2020, the DPC Investigator wrote to Tusla seeking submissions regarding the measures in place at the time of the breach to comply with Article 32 of the GDPR by reference to the principle set down in Article 5(1)(f) GDPR. The DPC Investigator also queried when Tusla's Privacy Policy and the document titled, *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"* were put in place.

2.8 On 2nd March 2020, Tusla responded with a submission document (**"the second submission"**) and the following documents: Tusla's Privacy Policy, Revision 1.5; Policy and Procedures for Responding to Allegations of Child Abuse and Neglect, dated September 2014; Tusla ICT Technical Controls, Document Version Number 1.01. The second submission also confirmed that Tusla's Privacy Policy and Policy & Procedures for Responding to Allegations of Child Abuse and Neglect were in place at the time of the breach.

2.9 On 19th March 2020, the DPC Investigator completed the final Inquiry Report and submitted it to me as decision-maker. I have considered the Inquiry Report and all relevant correspondence and submissions. Tusla was provided with my Draft Decision on 16th April 2020 and was afforded the opportunity to make submissions on the infringements that were provisionally identified therein and the corrective powers that I proposed to exercise. Tusla made submissions on 15th May 2020 and I have had regard

to those submissions. I have reached final 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.

3. The processing operation subject to this Decision

3.1 This Decision considers, inter alia, the level of security implemented by Tusla regarding its safeguarding letters at the time of the personal data breach. Article 32(1) of the GDPR obliges controllers to implement a level of security that is appropriate to its processing of personal data. This requires controllers to assess the risks presented by each of its processing operations and to implement measures appropriate to those risks.

3.2 A previous Decision of the DPC (Decision IN-19-10-1, dated 7th April 2020) found that Tusla had infringed Article 32(1) of the GDPR by failing to implement appropriate organisational measures in relation to the processing operations subject to that Decision. Those processing operations concerned Tusla's sharing of copies of medical records, social work files, and care plans with third parties. That Decision considered the risk of unauthorised disclosure of personal data arising from a failure to implement appropriate redaction in the documents.

3.3 The processing operation under consideration in this Decision concerns the issuing of safeguarding letters to third parties. This processing operation requires Tusla's staff to determine whether allegations are substantiated and whether it is necessary to inform a third party[1]. Where necessary, the social workers must write to the third party and determine what information to convey in that letter.

3.4 The safeguarding letter processing operation is distinct to the processing operations considered in Decision IN-19-10-1. Those processing operations concerned third party rights of access to pre-existing documents and the risk of a personal data breach if full redaction is not implemented. In the safeguarding letters, Tusla drafts letters to notify third parties of allegations of abuse. Redaction plays no role in safeguarding letters and this processing of personal data presents different risks, which may materialise through excessive personal data being included in the letters. Therefore, a separate risk analysis must inform the technical and organisational measures that Tusla was obliged to implement.

3.5 It follows that the finding of an infringement of Article 32(1) in Decision IN-19-10-1 is not indicative of an infringement regarding the safeguarding letter processing operation. Rather, this Decision must separately analyse the appropriate level of security and the security measures implemented by Tusla for this processing operation.

[1] Policy and Procedures for responding to Allegations of Child Abuse & Neglect at page 30.

4. Legal regime pertaining to the Inquiry and Decision

4.1 The General Data Protection Regulation 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 was given further effect in Irish law by the 2018 Act.

5. Materials considered

5.1 The DPC Investigator delivered the final Inquiry Report to me on 19th March 2020. I was also provided with all of the correspondence and submissions received in compiling the report, including:

i. The DPC's Final Inquiry Report, Inquiry Reference IN-19-12-8;
ii. The letter dated 11th December 2019 notifying Tusla of the commencement of the Inquiry;
iii. Breach notification form submitted 4th November 2019 (Breach Notification BN-19-11-81;
iv. Email correspondence between the DPC and Brendan Lyden of Tusla, dated 14th November 2019;
v. Redacted letter from Tusla to [redacted], dated 8th November 2019, [redacted] discuss the case;
vi. Redacted letter from Tusla to [redacted] dated 12th November 2019, regarding notice of the personal data breach;
vii. Redacted letter from Tusla to [redacted] of the safeguarding letter, dated 12th November 2019, seeking to contain the effects of the personal data breach;
viii. Tusla's Reponse to the DPC's Draft Inquiry Report (IN-19-12-08), v1.0, dated 21st February 2020;
ix. Tusla's data protection bulletin on breaches, dated 3rd April 2019;
x. Tusla's Second Submission on the DPC's Draft Inquiry Report (IN-19-12-08), v1.0, dated 2nd March 2020;
xi. Tusla's Privacy Policy, Revision 1.5, Approval date 18th May 2018;
xii. Tusla's Policy and Procedures for responding to Allegations of Child Abuse & Neglect, dated September 2014;
xiii. Tusla ICT Technical Controls, Version 1.01, which was last modified on 5th February 2020;
xiv. Tusla's Submission on the DPC's Draft Decision for Inquiry Ref: IN-19-12-08, dated 15th May 2020; and
xv. All other relevant correspondence between the DPC and Tusla.

5.2 I am satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout including, but not limited to, notifications to the data controller and opportunity for the data controller to comment on a draft Inquiry Report before it was submitted to me as decision-maker.

6. Data Controller

6.1 This Decision and the corrective powers contained herein are addressed to Tusla as the relevant data controller in relation to the findings made.

7. Personal Data

7.1 Personal data is defined under the GDPR as *"any information relating to an identified or identifiable natural person"*. The personal data breach identified in the Inquiry concerns the names of the data subjects and details of the abuse allegations. Thus, the data processed by Tusla includes personal data.

8. Analysis and findings

8.1 In its second submission, Tusla set out detailed proposed remedial actions to mitigate the risk of future breaches. This Decision makes findings as to whether infringements of the 2018 Act have occurred by reference to the date of the personal data breach. This Decision does not make findings as to the level of security provided by the proposed remedial actions or the actions taken by Tusla since the personal data breach. However, it is acknowledged that some of the issues leading to the findings in this Decision may have since been addressed by Tusla or may be in the process of being addressed.

A. Security of Processing

8.2 The personal data breach occurred because the social worker who sent the safeguarding letter did not know that the names and details of the allegations should not be included in the letter. In correspondence between Tusla and the DPC, Tusla submitted that:

> "The Tusla staff members believed that they were correct to release the information to [redacted] and believed they were following the Policy and Procedures for Handling Allegations of Child Abuse & Neglect."[2]

8.3 The final Inquiry Report took the view that sending the letter resulted in an infringement of Article 5(1)(f) of the GDPR, and that the incident also constituted an infringement of Article 32(1). In order to determine whether an infringement of Articles 5(1)(f) and 32(1) has occurred, it is necessary to analyse the technical and organisational measures that Tusla implemented at the time of the breach to ensure an appropriate level of security.

8.4 Article 5(1)(f) of the GDPR provides for the principle of integrity and confidentiality. It requires that data is processed in a manner that ensures appropriate security of the data

[2] Email correspondence between Tusla and the DPC, dated 14th November 2019 (Appendix D.2b of the final Inquiry Report).

using appropriate technical or organisational measures. The security of the personal data should protect against, *inter alia*, unauthorised or unlawful processing.

8.5 Article 32(1) of the GDPR elaborates on the requirement in Article 5(1)(f) to provide for security of processing:

> *"1. 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."*

8.6 In considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing. During the course of the Inquiry, Tusla informed the DPC Investigator that at the time of the breach it *"did not have a risk assessment framework in place to assess the risks of varying likelihood and severity associated with the forms of data processing at issue in the breach."*[3] This is an omission on Tusla's part. However, in order to assess whether there has been an infringement of Articles 5(1)(f) and 32(1) of the GDPR, this Decision must assess the risk presented by Tusla's processing of personal data at the time of the personal data breach. The technical and organisational measures that Tusla was obliged to implement are informed by the extent of the risk presented by its processing of personal data.

i. Assessing Risk

8.7 Tusla's functions require the processing of personal data regarding allegations of child abuse and neglect. As is evident from the Inquiry, in some instances, Tusla informs third parties of such allegations via safeguarding letters. Safeguarding letters may present a risk to the rights and freedoms of the complainants where the complainants are identified

[3] Tusla's Second Submission on the DPC's Draft Inquiry Report (IN-19-12-08), 2nd March 2020.

by, or identifiable to, the third party receiving the safeguarding letter. The technical and organisational measures that controllers and processors are obliged to implement must be appropriate to this risk.

8.8 Recital 76 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."*

8.9 Risk must be assessed objectively by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. Thus, the risk assessment must consider, first, the likelihood of complainants being identified to third parties, and, second, the severity of the risk to the rights and freedoms of the complainants by such an identification.

8.10 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[4] provides guidance as to the factors that should inform this risk assessment. In this case, the CJEU declared the Data Retention Directive[5] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court 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 retained, (ii) the sensitive nature of the data, and (iii) the risk of unlawful access. Regard must also be had to these factors in assessing the risk posed by the safeguarding letters processing operation.

8.11 The quantity of the personal data processed by Tusla in connection with its safeguarding letters is at the midpoint of the scale. Tusla's *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"*, at Section 27, makes clear that the allegations must be evaluated by a social worker to determine if they are substantiated. The personal data of the alleged abuser and the third party subject to the notification must also be processed as the policy requires the social worker to evaluate whether it is necessary to inform a particular third party and, if so, to also contact the alleged abuser to inform them of this.

8.12 The nature of the personal data processed by Tusla in connection with its safeguarding letters is highly sensitive. The personal data processed concerns allegations of child abuse

[4] 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).

[5] 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

and neglect. Unauthorised disclosure of this type of personal data has an inherent capacity to seriously infringe the rights and freedoms of complainants.

8.13 The risk of unlawful access to the personal data is high. Tusla uses its safeguarding letters to communicate certain information to third parties. This creates a high risk of unlawful access because, if the letters contain personal data that ought not to be disclosed, unlawful access would naturally follow. In addition to the type of personal data breach considered in the Inquiry, where the data subjects' names were included in the safeguarding letter, the risk of unlawful access also occurs where data subjects are indirectly identifiable based on details included in the letter, despite not being named therein. The risk is aggravated by the potential that individuals who receive safeguarding letters, who are outside the control of Tusla, might further disclose the personal data contained therein.

8.14 In assessing risk, regard must also be had to the scope, context and purposes of Tusla's processing of personal data in the safeguarding letters processing operation. The processing is undertaken to identify whether it is necessary to inform third parties of allegations and, if so, for communicating the allegations to specific third parties. Therefore, the specific scope of the processing of personal data for safeguarding letters is moderate. However, this must be balanced with the fact that Tusla has State-wide responsibility for improving wellbeing and outcomes for children and Tusla is likely to issue safeguarding letters on a State-wide basis.

8.15 The context of the safeguarding letters is significant in assessing the risk to rights and freedoms of data subjects. Safeguarding letters may to be issued parallel to criminal investigations by An Garda Síochána and criminal prosecutions brought by the Directors of Public Prosecutions. An inadequate level of security could have an adverse impact on such proceedings. This heightens the risk to the rights and freedoms of complainants.

8.16 The purpose of the processing is to ensure the ongoing safety of any child under the care and control of the relevant third party. This purpose may justify significant processing operations and the processing of sensitive personal data. This heightens the risk to the rights and freedoms of data subjects.

8.17 I find that there is a high risk, both in likelihood and severity, to the rights and freedoms of natural persons from Tusla's processing of personal data in connection with its safeguarding letters. I make this finding, in particular, in light of the high sensitivity of the data that is processed, the high risk of unlawful access to it, and the context that this processing of personal data takes place in. This risk relates to the possibility that complainants of child abuse and neglect could be identified or identifiable from the letters, and that excessive details concerning the allegations could be included. The high likelihood of this risk occurs due to the requirement that Tusla must, in some instances, share information on allegations with third parties, who are outside the control of Tusla. The high severity of the risk occurs due to the sensitivity of the personal data processed

by the social workers and the potential for material and non-material damage to vulnerable data subjects as a result of unlawful access to that personal data.

ii. Security measures implemented by Tusla

8.18 Tusla's first submission stated that *"this breach occurred as result of human error whereby the social worker did not show regard for the data protection provisions which are included in existing Tusla policies…"* It referenced Tusla's Privacy Policy and the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"*. It also stated that this policy would be replaced by the end of June 2020 by the Child Abuse Substantiation Procedure and Guidance Document. Tusla also appended a newscast on breaches that it issued internally to staff on 3rd April 2019. The newscast is relevant to this Decision's consideration of the data breach notification. However, as this document had not been issued at the time of the personal data breach, it is not relevant to considering Tusla's compliance with Articles 5(1)(f) or 32(1) of the GDPR for the purposes of this Decision.

8.19 Tusla's second submission, in replying to the DPC Investigator's letter of 24th February 2020, set out the measures that Tusla had in place at the time of the breach to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR. The second submission appended the documents referred to in the first submission, the Privacy Policy and the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"*. It also appended *"Tusla ICT Technical Controls"*, Version 1.01, which was last modified on 5th February 2020, but Tusla submits that it reflects the technical measures that were in place at the time of the breach. The second submission also stated that Tusla has a mandatory e-Learn in place for all staff at the time of this breach in order to raise awareness and train staff in data protection practices.

8.20 As decision-maker, I have had regard to the *'Tusla ICT Technical Controls'* document. I accept Tusla's submission that the measures outlined in this document were in place at the time of the breach. It outlines, inter alia, the information and community technology related security controls that Tusla had in place. It describes Tusla's ICT Security Charter and provides for the principle of confidentiality. The technical controls outlined include: physical access controls regarding access to Tusla's premises; logical access controls regarding access to Tusla's systems; network security to prevent unauthorised access to the network and undesirable traffic; endpoint security on Tusla's workstations, laptops and mobile devices; malware and email protection; encryption protocols; and software development procedures. The document also outlined that these controls are subject to assessment, including scanning of external systems every 6 months and penetration tests once a quarter. The document does not set out any organisational measures to address the risk of complainants being unnecessarily identified in safeguarding letters or of excessive details of the allegations being included in the letters.

8.21 I have also had regard to Tusla's Privacy Policy. The Privacy Policy expressly requires all staff, contractors and relevant third parties to ensure that the Policy is implemented and adhered to. It prohibits the processing of personal data that is not based on legislation to which Tusla is obliged to adhere or the consent of the data subject[6]. It provides that Tusla will implement appropriate technical and organisational measures[7]. Regarding, the principle of data minimisation, it provides that:

> *"Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation). Tusla will ensure that in designing methods of data collection, via whatever medium that only the personal data required to provide the benefit or service requested will be processed. Tusla will undertake regular reviews of the data requested to ensure that the amount of personal data collected is minimised.[8]"*

8.22 I have also had regard to the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"*. Section 27 of this document sets out the procedure for notifying a relevant third party of allegations of child abuse. It states that *"The social worker must…Determine what information will be conveyed to the relevant third party."* The document does not contain any guidance to social workers that would address the risk of complainants being unnecessarily identified in safeguarding letters or of excessive details of the allegations being included in the letters.

8.23 I note that Tusla staff believed that they were following the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"* when they identified the data subjects. That document also sets out a procedure for notifying alleged abusers of allegations against them. Section 20.5 provides that letters notifying alleged abusers should include the name of the complainant unless they wish to remain anonymous. Section 16.5 provides that *"It is the right of the alleged abuser to know who has made allegations against him or her so as to be able to make representations in the assessment process."* Safeguarding letters are inherently different to the letters provided for in Section 20.5 and assessing whether complainants need to be identified therein requires a separate analysis. Section 27 does not expressly distinguish safeguarding letters from other letters with regard to identifying complainants. The document's failure to do may have contributed to the staff's belief that they were following the policy and procedure when they included the data subjects' names and the details of the allegations.

iii. The appropriate level of Security

8.24 Having regard to the high risk presented by Tusla's safeguarding letters to the rights and freedoms of natural persons, I find that an appropriate level of security must include specific guidance to relevant Tusla staff on how the principle of data minimisation should

[6] At page 20.
[7] At page 26.
[8] At page 21.

apply to safeguarding letters. This guidance must ensure that pseudonymisation of personal data is implemented in the safeguarding letters wherever applicable. The guidance should also make it clear to relevant staff that the amount of personal data included should be limited to what is necessary for the purposes of the safeguarding letters. This guidance could have been achieved if the procedure for issuing safeguarding letters clearly provided for data minimisation and pseudonymisation. I have considered the security measures that Tusla implemented at the time of the breach; the nature, scope context and purposes of that processing; the cost of implementation; and the state of the art. I find that Tusla failed to implement appropriate organisational measures to provide such guidance.

8.25 The *'Tusla ICT Technical Controls'* document sets out ICT related technical security controls, but does not address the risk of a social worker, in good faith, working under the mistaken belief that it is necessary to identify a complainant in a safeguarding letter. Tusla's Privacy Policy generally provides for the principle of data minimisation, however it does not provide specific guidance on safeguarding letters. Furthermore, the policy focuses on data minimisation in the context of collecting personal data, but does not expressly reference sharing personal data with third parties.

8.26 Section 27 of the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"* sets out specific guidance for issuing safeguarding letters. However, this guidance does not incorporate data minimisation or pseudonymisation regarding the identity of complainants and other personal data. Rather, it simply states that the social worker must determine what information to convey. Further, the failure of the *"Policy and Procedures for responding to Allegations of Child Abuse & Neglect"* to distinguish safeguarding letters from other letters provided for in that document with regard to identifying complainants heightens the risk that complainants might be unnecessarily identified. Although Tusla submitted that it had a mandatory GDPR e-Learn in place for all staff at the time of the breach, the inquiry found no evidence of training that provides the required specific guidance for safeguarding letters.

8.27 I have had regard to the cost of implementing organisational measures that would provide specific guidance to social workers on the principle of data minimisation and pseudonymisation in safeguarding letters. I find that implementing such measures, for example through an updated procedure for issuing safeguarding letters, would not impose a disproportionate cost on Tusla with regard to their obligation to implement a level of security appropriate to the risk presented. However, it should be noted that implementing such specific guidance does not relieve Tusla of its obligation to continually evaluate the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by the processing of personal data in safeguarding letters.

iv. Finding

8.28 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate organisational measures to ensure a level of security appropriate to the risk presented

by its safeguarding letters processing operation. The measures that ought to have been implemented include specific guidance to relevant Tusla staff ensuring data minimisation and pseudonymisation in safeguarding letters where appropriate.

B. Data Breach Notification

8.29 The safeguarding letter was sent on 15th March 2019 and [redacted] contacted Tusla about the letter on 12th April 2019. Tusla notified the DPC of the breach on 4th November 2019, over 29 weeks after the data subjects complained. In the data breach web form, Tusla explained the reason for the delay as follows:

> *"This incident was confirmed as a breach following a report to the Data Protection Unit on 31/10/2019."*

8.30 In correspondence with the DPC, dated 14th November 2019, Tusla elaborated on that reason as follows:

> *"The Tusla staff members believed that they were correct to release the information* [redacted] *and believed they were following the Policy and Procedures for Handling Allegations of Child Abuse & Neglect. It was only following the receipt and investigation of complaint from the data subjects about this matter that the local office determined to refer to the DPU."*

i. Analysis

8.31 Article 33(1) of the GDPR provides:

> *'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.'*

8.32 The personal data breach created a risk to the rights and freedoms of the data subjects. The personal data that was disclosed concerns [redacted]. Unauthorised disclosure of this type of personal data has an inherent capacity to seriously infringe the rights and freedoms of complainants. The likelihood of the damage to the data subjects is aggravated by the fact that the letter was subsequently [redacted] Accordingly, Tusla was obliged to notify the DPC of the breach without undue delay and, if feasible, within 72 hours of becoming aware of the breach.

8.33 The requirement to notify without undue delay under Article 33(1) must be assessed from when Tusla became aware of the personal data breach. The Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679[9] provide that:

> *"WP29 considers that a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."*[10]

8.34 The Guidelines go on to consider cases where there is uncertainty as to whether a personal data breach has occurred:

> *"In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required."*[11]

8.35 I accept that the staff who sent the safeguarding letter were unaware at the time of sending the letter that it would result in a personal data breach. However, when the data subjects complained, Tusla was on notice of a potential personal data breach. This necessitated prompt action from Tusla to determine whether a personal data breach had occurred. Therefore, I find that Tusla became aware of the personal data breach on the date of the complaint, 12th April 2019.

8.36 Tusla's failure to notify the DPC of the personal data breach until 4th November 2019 constitutes an undue delay. A period of 29 weeks from when Tusla became aware of the breach is grossly excessive and there are no circumstances concerning this breach that justify a failure to notify the DPC within 72 hours of the complaints. Tusla's explanation, that the staff members who issued the letters believed that they were correct to release the information, does not justify this delay because, after receiving the complaints, there was an obligation to investigate promptly and determine whether a personal data breach had occurred. In this regard, I note that Tusla's Privacy Policy requires that all potential data breaches are notified to their Data Protection Unit as soon as they become aware of same[12]. I also note that the newscast, circulated to staff internally on 3rd April 2019, reemphasises this message that Tusla. However, Tusla did not follow its own Privacy Policy in this instance, and this resulted in an infringement of Article 33(1) of the GDPR.

[9] Article 29 Working Party, Guidelines on Personal Data breach notification under Regulation 2016/679, Adopted 6 February 2018.
[10] Ibid at page 10.
[11] Ibid at page 11.
[12] At page 28.

ii. Finding

8.37 I find that Tusla infringed Article 33(1) of the GDPR by failing to notify the DPC of the personal data breach without undue delay.

9. Corrective Powers

9.1 Having carefully considered the infringements identified in this Decision, 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, having considered all of the corrective powers set out in Article 58(2):

a) Article 58(2)(b) - the issue of reprimands to Tusla in respect of its infringements of Article 32(1) and 33(1) of the GDPR;
b) Article 58(2)(d) – order Tusla to bring its processing into compliance with Article 32(1) of the GDPR; and
c) Article 58(2)(i) – the imposition of an administrative fine, pursuant to Article 83, in respect of Tusla's infringements of Articles 32(1) and 33(1) of the GDPR.

A. Reprimands

9.2 I now issue Tusla with reprimands under Article 58(2)(b) of the GDPR regarding its infringements of Article 32(1) and Article 33(1) of the GDPR respectively. This is in circumstances where Tusla failed to implement a level of security appropriate to the risk presented by its safeguarding letter processing operation, as required by Article 32(1), and failed to notify the DPC of the personal data breach without undue delay, as required by Article 33(1).

B. Order to Tusla to bring its processing into compliance with Article 32(1) of the GDPR

9.3 In addition to the Reprimand in respect of the infringement of Article 32(1), in accordance with Article 58(2)(d) of the GDPR, I order Tusla to bring its safeguarding letter processing operation into compliance with Article 32(1) of the GDPR by implementing appropriate organisational measures to ensure a level of security appropriate to the risk. Tusla should perform a risk assessment to inform the measures that it must implement. The measures should include specific guidance to relevant Tusla staff ensuring data minimisation and pseudonymisation in safeguarding letters where appropriate. However, the manner of implementation of compliance is a matter for Tusla to decide.

9.4 In determining the time scale for Tusla to comply with this order by implementing appropriate organisational measures, I have had regard to Tusla's submissions on the

Draft Decision. Those submissions detailed some of the challenges faced by Tusla surrounding the current Covid-19 crisis, including the delivery of critical services to children and families during the Covid-19 pandemic and the need to redeploy staff who are integral to the implementation of Tusla's action plan with regard to the specific processing activity of providing safeguarding letters to third parties.

9.5 The "Policy & Procedures for Responding to Allegations of Child Abuse & Neglect", dated September 2014, is due to be replaced by a Child Abuse Substantiation Procedures Document, but this will likely be deferred until March 2021 as a result of Covid-19. In the meantime, Tusla proposes to develop and issue a guidance document for all relevant social worker and business support staff, which sets out specific steps and practical guidance for staff to apply when issuing safeguarding letters to third parties. Tusla's target completion date for this guidance is 30th June 2020. I accept that implementing new Child Abuse Substantiation Procedures is a significant undertaking for Tusla, which includes complex considerations that exceed the scope of this Decision. I acknowledge that replacing the document from 2014 must be done in coordinated manner. However, it is significant that the Tusla staff who issued the letter considered in this Decision believed that they were following the "Policy and Procedures for responding to Allegations of Child Abuse & Neglect" when they [redacted] and that the document does not expressly distinguish safeguarding letters from other letters with regard to identifying complainants. However, I note that Tusla aims to update both the 2014 document and the Child Abuse Substantiation Procedures by 30th November 2020. In light of the detailed action plan submitted by Tusla, and the guidance document that it proposes to issue by 30th June 2020, I am satisfied that the timeline proposed by Tusla is reasonable in the particular circumstances. Therefore, I order Tusla to bring its safeguarding letter processing operation into compliance with Article 32(1) of the GDPR by **1st December 2020.** However, in the meantime, I direct that Tusla must take steps to alert all relevant staff to the issue that arose in this case so that, in advance of the formal processes for safeguarding letters being updated by December 2020, staff at Tusla are on notice of the consideration they must give to the appropriate protection of the data of complainants who contact Tusla to allege abuse at the hands of a third party. On or before December 2020, Tusla must submit a report to the DPC outlining the steps it has taken in respect of the formal process update it is preparing and by **15th June 2020** must submit a confirmation report that it has put relevant staff on notice of the issues that must immediately be addressed by reference to this Decision. [redacted]

C. Administrative Fine

9.6 In addition to the corrective powers under Article 58(2)(b) & (d), I also impose an administrative fine on Tusla for its infringements of Article 32(1) and Article 33(1).

i. Decision to impose an Administrative Fine

9.7 In order to determine whether an administrative fine should be imposed under Article 58(2)(i) GPDR, and to decide on the value of the fine if applicable, I must give due regard to the criteria set out in Article 83(2) GDPR:

'2. 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.'

9.8 I will now proceed to consider each of these criteria in turn in respect of Tusla's infringement of Articles 32(1) and 33(1) of the GDPR:

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;

9.9 The nature of the infringement of Article 32(1) must be assessed in light of the fact that infringements of Article 32 are usually capped at the lower threshold under Article 83(4), suggesting that infringements of Article 32, depending on the circumstances, may be less serious in nature than infringements that evoke higher threshold under Article 83(5) (despite the fact that such caps are not applicable in the circumstances where Section 141 of the 2018 Act applies). However, the nature of the failure to implement appropriate organisational measures must also be assessed in light of the high sensitivity of the personal data processed. Furthermore, the fact that Tusla has State-wide responsibility for improving wellbeing and outcomes for children means that a large number of data subjects could potentially be affected by the lack of appropriate security. The high sensitivity and the potentially large number of data subjects significantly elevates the seriousness of the nature of the infringement of Article 32(1).

9.10 The nature of the infringement of Article 33(1) must also be assessed in light of the fact that it is also usually capped at the lower threshold under Article 83(4). However, the nature of this infringement must also be assessed in light of the purpose of Article 33(1), which is to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded to the extent possible by mitigating the risks to them arising from a data breach, by action on the part of the supervisory authority[13], for example ordering a controller to communicate a personal data breach to affected data subjects under Article 58(2)(e) of the GDPR. The personal data breach concerned vulnerable data subjects and highly sensitive personal data. In those circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the infringement of Article 33(1) is serious in nature.

9.11 The gravity of the infringement of Article 32(1) is serious in circumstances where it directly resulted in the personal data breach. There were [redacted] affected by the personal data breach. Each data subject has lost significant control over their personal data. The safeguarding letter has been [redacted] and it is not possible to identify how many individuals the letter has been disclosed to. I consider that the likely

[13] Recital 85 GDPR.

level of damage suffered by the data subjects as a result of the breach is high and that their rights and freedoms have been seriously infringed.

9.12 The gravity of the infringement of Article 33(1) is serious in circumstances where it resulted in a failure on the part of Tusla to mitigate the personal data breach. Tusla notified the DPC of the personal data breach over 29 weeks after receiving the complaints from the data subjects. It was not until after this notification that Tusla attempted to retrieve the safeguarding letter and to request that [redacted] Furthermore, it was not until after the 29 weeks had elapsed the Tusla contacted the data subjects in relation to the breach. One of the [redacted] was likely unaware of the breach during the 29 week period.

9.13 Regarding the duration of the infringement of Article 32(1), it is significant that the breaches occurred on 15th March 2019 and that the Policy and Procedures for Responding to Allegations of Child Abuse and Neglect have been in place since September 2014. In those circumstances, it is clear that the infringement of Article 32(1) commenced at the enactment of the GDPR in May 2018 and was ongoing at the time of the personal data breach. Therefore, the duration of the infringement, for the purposes of this Decision, is over 9 months in length.

9.14 Regarding the duration of the infringement of Article 33(1), as outlined above, there are no circumstances concerning this breach that justify a failure to notify the DPC within 72 hours of becoming aware of it. Therefore, the infringement commenced on 15th April 2019, 72 hours after Tusla became aware of it. The infringement ceased when Tusla notified the DPC on 4th November 2019. Therefore, the duration of this infringement is exactly 29 weeks in length. I find the duration of this infringement is at the highest end of the scale of culpability in the circumstances.

b) ***the intentional or negligent character of the infringement;***

9.15 I find that Tusla's infringements were unintentional, but that they were negligent in character. The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 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."*[14]

9.16 Tusla was negligent and breached the duty of care required of it by omitting to carry out a risk assessment to assess the risks of varying likelihood and severity associated with processing of personal data in safeguarding letters and in failing to implement a level of

[14] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

security appropriate to that risk. However, I am satisfied that Tusla did not intend to cause this infringement. Tusla was highly negligent in the extent of its infringement of Article 33(1). However, I am satisfied that the 29 week delay in notifying the DPC was not caused with knowledge or wilfulness of infringing Article 33(1).

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

9.17 Tusla took action to mitigate the damage suffered by the data subjects as a result of the personal data breach. On 12th November 2019, it wrote to the [redacted] apologising for and providing information regarding the breach. Tusla wrote to the [redacted] data subject, [redacted]. Tusla also wrote to the recipient of the safeguarding letter to seek to retrieve it and to request that the [redacted]. However, these attempts were unsuccessful. Furthermore, all of the Tusla's mitigating action was taken after the 29 week delay. This delay reduced the capacity of Tusla's action to mitigate the damage suffered by the 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;***

9.18 Regarding the infringement of Article 32(1), as outlined in part 8(A) of this Decision, Tusla did not implement appropriate organisational measures pursuant to Article 32(1). I consider that Tusla 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 an infringement of Article 32(1) against Tusla, this factor cannot be considered aggravating in respect of that infringement.

9.19 Regarding the infringement of Article 33(1), I note that Tusla's Privacy Policy requires that all potential data breaches are notified to their Data Protection Unit as soon as they become aware of same. Although this Policy was negligently not followed by Tusla staff in this case, I find that the existence of this organisational measure is mitigating in the circumstances.

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

9.20 A previous Decision of the DPC *(*Decision IN-19-10-1, dated 7th April 2020) found that Tusla infringed Articles 32(1) and 33(1) of the GDPR. As outlined in Part 3 above, that Decision concerned the risk of unauthorised disclosure of personal data arising from a failure to implement appropriate redaction in documents shared by Tusla with third parties and Tusla's failure to implement appropriate organisational measures in relation to that risk. Tusla also did not carry out a risk assessment in respect of that risk. The personal data breaches considered in that Decision occurred between 14th November 2018 and 14th March 2019.

9.21 Decision IN-19-10-1 also found that Tusla had infringed Article 33(1) of the GDPR by notifying the DPC of one of the personal data breaches 2 days after the 72 hour period provided for in Article 33(1) had expired. That infringement occurred from 26th May 2019 – 28th May 2019. Therefore, it occurred during the 29 week period under consideration in this Decision, but concluded before the conclusion of the infringement under consideration in this Decision. The infringements of Articles 32(1) and 33(1) in Decision IN-19-10-1 are relevant to this Decision as indicate a systemic nature of Tusla's failure to comply with Articles 32(1) and 33(1) at the time of the breaches.

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

9.22 After the breach was notified to the DPC, Tusla cooperated fully to remedy the infringements and to mitigate their adverse effects. Regarding the infringement of Article 32(1), in response to the personal data breach, Tusla issued a formal memo to social work staff about considerations necessary when sharing information with third parties. It is developing a Child Abuse Substantiation Procedure and Guidance Document, which is due to be implemented in June 2020, and which will contain specific instruction with regards to sharing safeguarding information with third parties. Tusla is also implementing additional staff training specific to the data protection issues uncovered in the Inquiry. In its submissions dated 15th May 2020, Tusla set out a detailed action plan that was developed and agreed by Tusla's Senior Leadership Team in response to the specific issues identified in this inquiry.

9.23 Regarding the infringement of Article 33(1), in its first submission to the DPC, Tusla undertook to update and circulate the breach newscast to staff, to scope further staff training needs, and to issue a formal memo from the Senior Leadership Team reminding staff, inter alia, of the need to notify the DPC of personal data breaches within 72 hours. In its submissions dated 15th May 2020, Tusla stated that a formal memo will be issued to all staff by 29th May 2020.

g) ***The categories of personal data affected by the infringement;***

9.24 The categories of personal data affected by the infringements are highly sensitive. Unauthorised disclosures of allegations of child abuse and neglect is likely to cause immediate damage and distress to complainants. This is aggravating in respect of both the infringement of Article 32(1) and of Article 33(1). The infringement of Article 32(1) is aggravated because resulting personal data breaches are likely to cause more damage to the rights and freedoms of data subjects where the personal data compromised is highly sensitive. The infringement of Article 33(1) is aggravated because the higher risk to the rights and freedoms of data subjects makes prompt notification to the DPC even more imperative.

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;***

9.25 The infringements became known to the DPC because Tusla notified the DPC of the personal data breach. Tusla's compliance with its own obligation to notify personal data breaches under Article 33 cannot be considered mitigating in respect of the Article 32(1) infringement. Conversely, the undue delay when notifying the DPC of the breach is not aggravating in circumstances where that infringement is the subject of consideration for this corrective power.

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;***

9.26 Corrective powers have not previously been ordered against Tusla with regard to the subject matter of this Decision. Although corrective powers were exercised in Decision IN-19-10-1, those corrective powers concerned different processing operations and therefore are not concern the same subject matter as this Decision.

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

9.27 Not Applicable.

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.***

9.28 In its submissions dated 15th May 2020, Tusla requested that the administrative fine be as close to the minimum amount on that range as possible due to, amongst other things, the administrative fine already imposed by the DPC in Decision IN-19-10-1, dated 7th April 2020. While Tusla's previous infringements are aggravating in accordance with Article 83(2)(e), in the circumstances, the administrative fine that has already been imposed is relevant to determining what is effective, proportionate and dissuasive. As noted by the Article 29 Working Party:

> *"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)."*

9.29 Since Inquiries IN-19-10-1 and IN-19-12-8 commenced, Tusla has taken significant steps to bring its processing operations into compliance with the GDPR. The personal data breach considered in this Decision occurred shortly after the personal data breaches considered in Decision IN-19-10-1. Although each Decision considers distinct processing operations, I find it mitigating that Tusla has already taken steps to address the systemic issues leading to delays in notifying personal data breaches and that a fine has been imposed on Tusla in respect of another infringement Article 33(1) that occurred at a similar time to this infringement.

9.30 I find that an administrative fine should be imposed in respect of both the infringement of Article 32(1) and the infringement of Article 33(1) in addition to the exercise of other corrective powers under Article 58(2). In coming to this conclusion, I have had due regard to factors a – k above and the need to deter non-compliance in a proportionate manner. I have taken factors a – k into account when calculating a fine that is effective, proportionate and dissuasive, as required by Article 83(1) of the GDPR.

ii. Calculating the Administrative Fine

9.31 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 Tusla with the opportunity comment in accordance with fair procedures. Tusla submitted that the administrative fine should be as close to the minimum amount on the proposed range as possible due to: the necessity of Tusla to deploy its resources to the delivery of its vital services as the Child and Family Protection Agency for the State; the value of using that resource as a contribution towards implementing the proposed corrective measures; the continued efforts and commitment already provided by Tusla to the DPC to address the systemic issues which are the subject matter of this and other DPC inquiries; and the administrative fine already accepted by Tusla for the 3 x Breach Inquiry (ref. IN-19-10-01). This Decision has had due regard to those factors in calculating the fine.

9.32 Article 83(3) of the GDPR provides that:

> *'If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.'*

9.33 Therefore, when calculating the administrative fine in respect of Tusla's infringements of Articles 32(1) and 33(1), I am obliged to ensure that the total amount of that fine does not exceed the amount specified for the gravest infringement. I consider that both infringements are serious in nature. However, in light of the grossly excessive period of 29 weeks that Tusla took to notify the DPC of the personal data breach, contrasted with the moderate scope of Tusla's safeguarding letter processing operation, I find that Tusla's infringement of Article 33(1) is the gravest infringement in the circumstances. Therefore, in calculating the administrative fine, I have had regard to this infringement only. The

infringement of Article 32(1) is not considered aggravating for the purposes of calculating the fine.

9.34 The weight to be given to the factors in Article 83(2)(a) to (k) and their impact on the amount of the fine are matters for the supervisory authority's discretion. The expression *"due regard"* provides the supervisory authority with a broad discretion in this respect. In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[15].

9.35 The methodology that I have followed in calculating the administrative fine is as follows. The first step in calculating the administrative fine is to locate the infringement on the permitted range in terms of its seriousness taking into account any aggravating circumstances and arriving at an appropriate fine for the infringement. The second step is to apply any mitigating circumstances to reduce the fine where applicable. Finally, in accordance with Article 83(1) of the GDPR, it is necessary to consider whether the figure arrived at is "*effective, proportionate and dissuasive*" in the circumstances.

9.36 The permitted range for this administrative fine is set out in Section 141(4) of the 2018 Act[16]. The fine shall not exceed €1,000,000 because Tusla is a public authority[17] that does not act as an 'undertaking' within the meaning of the Competition Act 2002[18]. Taking into account the seriousness of the infringement and the aggravating factors, the infringement must be located on this scale of zero to €1,000,000. I consider that the figure of **€120,000** reflects the seriousness of this infringement and the aggravating factors. This figure is intended to reflect, in particular, the duration of the infringement, as set out in accordance with Article 83(2)(a), and the consequences of the infringement. In particular, how the infringement resulted in a significant delay in one of the data subjects being notified of the personal data breach and a delay in implementing mitigating measures to address the high level of damage that the data subjects are likely to have suffered. I have also had regard to the fact that Tusla has previously infringed Article 33(1), in accordance with Article 83(2)(e), and that this is indicative of a systemic failure to comply with the notification requirements under Article 33(1). Finally, I have had regard to the highly

[15] See by analogy Electrabel v Commission, T 332/09, ECLI:EU:T:2012:672, para 228, Marine Harvest ASA v Commission, T-704/14, ECLI:EU:T:2017:753, para 450.

[16] Section 141(4) provides:
"*Where the Commission decides to impose an administrative fine on a controller or processor that—*
(a) is a public authority or a public body, but (b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002 , the amount of the administrative fine concerned shall not exceed €1,000,000."

[17] Public authority is defined in Section 2 of the 2018 Act as including "*any other person established by or under an enactment (other than the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act)*". Tusla was established pursuant to Section 7 of the Child and Family Agency Act 2013 and, thus, is a Public authority within the meaning of the 2018 Act.

[18] Undertaking is defined in Section 3 of the Competition Act 2002 as "*a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service*". As Tusla does not provide its services for a gain, it is not an undertaking within the meaning of that Act.

sensitive categories of personal data affected by the infringements, pursuant to Article 83(2)(g).

9.37 I consider that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(b), 83(2)(c), 83(2)(d), and 83(2)(f) of the GDPR mitigating. To take account for the unintentional character of the infringement, I have reduced the fine by **€12,500** in accordance with Article 83(2)(b). To account for the action taken by Tusla to mitigate the damage suffered by the data subjects, all of such action was taken after a significant delay which reduced the mitigating effect, I have reduced the figure by **€10,000** in accordance with Article 83(2)(c). To account for the organisational measures that Tusla had in place in its Privacy Policy at the time of the infringement with regard to its Article 33(1) notification obligations, I have reduced the figure by **€12,500** in accordance with Article 83(2)(d). To account for the cooperation that Tusla engaged with the DPC to remedy the infringement, I have reduced the figure by **€25,000** in accordance with Article 83(2)(f). In light of the fine already imposed on Tulsa in Decision IN-19-10-1 and the requirement that fines be effective, proportionate and dissuasive, I have reduced the figure by **€20,000** in accordance with Article 83(2)(k). Thus, the total figure for reducing the fine in light of the mitigating factors is **€80,000**. Applying the mitigating factors, the figure for the administrative fine is **€40,000**.

9.38 I must consider this figure in light of the requirement in Article 83(1) that administrative fines shall be "*effective, proportionate and dissuasive*". I coming to this Decision, I have considered 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. I note that Tusla has an operational budget of over €750 million. As decision-maker for the Commission, I consider it important to strongly discourage the activity involved in this infringement and to encourage the prompt notification of the DPC under Article 33(1) where relevant. I am of the view that when calculating a fine that is effective, proportionate and dissuasive, the fine must have a significant element of deterrence, particularly in respect of serious infringements, such as the infringement in issue. Having regard to the foregoing, I consider that the final figure of **€40,000** meets the requirements of effectiveness, proportionality and dissuasiveness in respect of the infringement and data controller in issue. This amounts to **0.0053%** of Tusla's operational budget, or **4%** of the cap available.

10. Right of Appeal

10.1 This Decision is issued in accordance with Sections 111 of the 2018 Act. Pursuant to Section 150(5) of the 2018 Act, Tusla has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is received by it.

Helen Dixon
Commissioner for Data Protection