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-19-10-1

Commission Decision-Maker:

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

Date of Decision: 7th April 2020

Contents

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 conducted by Authorised Officers of the Data Protection Commission. The Authorised Officers 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 Section 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 20th February 2019, Tusla notified the DPC of a personal data breach ("**the first breach**") via the Data Protection Commission's personal data breach web form (Breach Notification BN-19-2-261). This breach occurred when Tusla [redacted] The breach occurred on 14th November 2018 and Tusla became aware of it on 18th February 2019. [redacted] Tusla stated in the personal data breach web form that [redacted] should have been redacted. It is outside the scope of this Decision to consider the [redacted] for the purposes of this decision, I accept Tusla's submission concerning the requirement for confidentiality [redacted] The breach came to Tusla's attention when [redacted] Tusla notified the data subjects of the breach via telephone. In response to the breach, Tusla's social work department undertook to risk assess and plan for any communications concerning the [redacted] Tusla also sent [redacted] should be sent via the social work team.

2.2 On 22nd March 2019, Tusla notified the DPC of a personal data breach ("**the second breach**") via the Data Protection Commission's personal data breach web form (Breach Notification BN-19-3-371). This breach occurred when Tusla unintentionally provided an individual who was [redacted] The breach occurred on 14th March 2019 and Tusla became

aware of it on 20th March 2019. [redacted] The breach occurred when the [redacted] The Appeals Panel was provided with three copies of the social work file. The file was redacted, but in error, one document with the address and phone number was not redacted. The Appeals Panel provided the file with this document to the [redacted] Tusla subsequently [redacted] They also liaised with the data subjects, Gardai and the local council concerning security, alternative housing, and school supports.

2.3 On 28th May 2019, Tusla notified the DPC of a personal data breach ("**the third breach**") via the Data Protection Commission's personal data breach web form (Breach Notification BN-19-5-486). This breach occurred when Tusla unintentionally provided the [redacted] The breach occurred on 27th January 2019 and Tusla became aware of it on 23rd May 2019. Tusla provided the [redacted] authorised to receive. However, the address, contact details, and school location should have been redacted. [redacted] Tusla contacted [redacted] asked her to destroy the care plan and to ensure that it is not shared with other people. Tusla also contacted and advised the [redacted] to be vigilant and to report any further events to the social work team.

2.4 On 24th October 2019, the Authorised Officers 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 breaches identified above. The letter informed Tusla that the Inquiry would examine whether or not Tusla had discharged its obligations in connection with the breaches 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 32 and 33 of the GDPR.

2.5 On 28th November 2019, the Authorised Officers issued the draft Inquiry Report to Tusla. The draft Inquiry Report set out the Authorised Officers' 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 draft Inquiry Report by 27th December 2019. The Authorised Officers informed Tusla that they would consider any such submissions before proceeding to finalise the Inquiry Report. Tusla requested an extension of the deadline to 27th January 2020. The Authorised Officers agreed to extend the deadline to 16th January 2020, which was later further extended to 20th January 2020.

2.6 On 21st January 2020, Tusla sent its submissions on the draft Inquiry Report to the Authorised Officers. The Authorised Officers analysed the contents of the submissions and modified the report to correct one factual inaccuracy. In the view of the Authorised Officers, none of the remainder of the submissions required a material change to the report.

2.7 On 14th February 2020, the Authorised Officers wrote to Tusla, issuing a number of follow up questions concerning the measures that Tusla had in place at the time of the breaches to

comply with Article 32 of the GDPR by reference to the principle set down in Article 5(1)(f). Tusla responded on 21st Febraury 2020 with the submission document, titled '*Tusla's Second Submission on the DPC's Draft Inquiry Report (IN-19-10-01)*', dated 21st Febraury 2020. The following documents were appended to the submission: Tusla ICT Technical Controls, Version 1.01; and Tusla's submissions on DPC Inquiry Initiated in December 2018, Ref IN 18-11-000004, Version 1.0, dated 13th February 2019.

2.8 On 24th February 2020, the Authorised Officers 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 12th March 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 2nd April 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. Legal regime pertaining to the Inquiry and the Decision

3.1 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.

4. Materials considered

4.1 The Authorised Officers delivered the final Inquiry Report to me on 24th February 2020. I was also provided with all of the correspondence and submissions received in compiling the report, including:

i. The letter dated 24th October 2019 notifying Tusla of the commencement of the Inquiry;
ii. Breach notification form submitted 20th February 2019 (BN-19-2-261);
iii. Email correspondence between the DPC and Brendan Lyden of Tusla, dated 20th February 2019, 1st March 2019, and 20th March 2019;
iv. Breach notification form submitted 22nd March 2019 (BN-19-3-371);
v. Email correspondence between the DPC and Brendan Lyden of Tusla, dated 22nd March 2019, 1st April 2019, 12th April 2019, 24th April 2019, 20th May 2019, 22nd May 2019, 23rd May 2019, and 24th May 2019;
vi. Email correspondence between the DPC and Danielle Dunican of Tusla, dated 5th June 2019 and 7th June 2019;
vii. Tusla's data protection incident report dated 22nd May 2019;
viii. Letter to Tusla from [redacted] date redacted but received by the Data Protection Commission on 29th March 2019(redacted);

ix. Letter to Tusla from [redacted] dated 15th March 2019 (redacted);
x. Letter to Tusla from [redacted] dated 14th March 2019 (redacted);
xi. Letter dated 22nd March 2019 from Tusla to [redacted] (redacted);
xii. Letter dated 22nd March 2019 from Tusla to [redacted] (redacted);
xiii. Tusla's Policy and Procedures for Responding to Allegations of Child Abuse & Neglect, dated September 2014;
xiv. Breach notification form concerning the third breach submitted 28th May 2019;
xv. Email correspondence between the DPC and Brendan Lyden of Tusla, dated 29th May 2019 and 3rd July 2019;
xvi. Tusla's response to the Draft Inquiry Report dated 21st January 2020;
xvii. Tusla's Data Protection Bulletin (Newscasts and Posters);
xviii. Tusla's Screening and Risk Assessment Guidance (V0.4);
xix. Tusla's Second Submission on the DPC's Draft Inquiry Report (IN-19-10-01)', dated 21st Febraury 2020;
xx. Tusla ICT Technical Controls, Version 1.01;
xxi. Tusla's submissions on DPC Inquiry initiated in December 2018, Ref IN 18-11-000004, Version 1.0, dated 13th February 2019;
xxii. Tusla's Submission on the DPC's Draft Decision for Inquiry Ref: IN-19-10-01, Version 1.0, dated 2nd April 2020;
xxiii. Tusla's Detailed Action Plan, dated 31st March 2020; and
xxiv. All other relevant correspondence between the DPC and Tusla.

4.2 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.

5. Data Controller

5.1 This Decision and the corrective measures that are proposed herein are addressed to Tusla as the relevant data controller in relation to the findings made.

6. Personal Data

6.1 'Personal data' is defined under the GDPR as *'any information relating to an identified or identifiable natural person'*. The personal data breaches identified in the Inquiry concern addresses, school location, and contact details of natural persons who are identifiable from the information in question. Thus, the data processed by Tusla includes 'personal data'.

7. Analysis and findings

7.1 Since the Inquiry commenced, Tusla has taken steps to address some of the issues identified in the Inquiry. This Decision makes findings as to whether infringements of the 2018 Act have occurred by reference to the dates of the personal data breaches (even if those infringements have since been addressed) or are occurring. Therefore, it is acknowledged that some of the issues leading to the findings in this Decision may have since been addressed by Tusla.

A. Security of Processing

7.2 The three personal data breaches identified in the Inquiry resulted from Tusla's failure to redact personal data when providing documents to third parties. Tusla identified the causes of the confidentiality breaches as employee error or omission. The final Inquiry Report took the view that Tusla's notification of the breaches to the DPC was an admission that it had infringed Articles 5(1)(f) and 32 of the GDPR. This Decision finds that a notification of a personal data breach is not *per se* an admission of an infringement of Articles 5(1)(f) or 32 of the GDPR. Rather, this Decision's consideration of whether any such infringements have occurred is based on an analysis of the appropriateness of the technical and organisational measures that Tusla implemented at the time of the breaches to ensure an appropriate level of security.

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

7.4 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.'

7.5 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.

i. Assessing Risk

7.6 The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the processing. Article 32(2) of the GDPR expressly states that the risk of unauthorised disclosure should be considered when assessing the appropriate level of security. Regarding Tusla's processing of personal data, a risk of unauthorised disclosure includes where it shares documents containing personal data with third parties. In such circumstances, Tusla relies on comprehensive redaction to protect the rights and freedoms of data subjects.

7.7 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.'

7.8 It is necessary to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. In Tusla's case, this risk assessment must have particular regard to the risk of an unauthorised disclosure of personal data to third parties. Thus, the risk assessment must consider, first, the likelihood of such a disclosure occurring, and, second, the severity of the risk to the rights and freedoms of natural persons.

7.9 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[1] provides guidance as to the factors that should inform this risk assessment. In this case, the CJEU declared the Data Retention Directive[2] 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

[1] 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).

[2] 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

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. In assessing the risk posed by Tusla's processing, regard must also be had to these factors.

7.10 Tusla processes a vast quantity of personal data on data subjects. It estimated that it would receive 60,000 child protection reports, 6,000 referrals and 8,000 school absence reports in 2019. It is clear from the personal data breaches identified in the Inquiry that it also processes medical records, addresses, contact details, social work files, and care plans in respect of its data subjects. Each category of documents that Tusla processes is likely to contain a significant amount of personal data on any given data subject.

7.11 The personal data processed by Tusla is especially sensitive in some instances. The data is likely to include special category data pursuant to Article 9 of the GDPR in some instances, for example the medical reports identified in the first breach. Furthermore, other data that Tusla processes is also particularly sensitive, for example the [redacted]

7.12 There is a significant risk of unlawful access arising from Tusla's processing. As is evident from the three personal data breaches identified in the Inquiry, Tusla's processing includes the transfer of personal data to third parties in some instances. The personal data that can be disclosed to third parties is dependent on a case by case analysis, with redaction playing an essential role in protecting the rights and freedoms of data subjects. In those circumstances, there is a high risk of unlawful access to personal data in the absence of appropriate technical and organisational measures to ensure comprehensive redaction.

7.13 I find that Tusla's processing of personal data presents a high risk, both in likelihood and severity, to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons manifests, in particular, in the risk of unlawful or unauthorised disclosure of personal data to third parties. The likelihood of this risk must be categorised as high due to the quantity of data processed and how that processing includes transferring personal data to third parties.

7.14 The severity of the risk to the rights and freedoms of the natural persons arising from such unlawful or unauthorised disclosure is also high. The high severity of this risk flows from the sensitive nature of the personal data that is processed and the context and purposes of the processing. Tusla's functions include, amongst other functions, providing for the protection and care of children; care and protection for victims of domestic, sexual or gender-based violence; and services relating to the psychological welfare of children and their families[3]. Unauthorised disclosures of personal data that is processed in the context of such functions pose a significant risk to the rights and freedoms of vulnerable data

[3] Section 8 of the Child and Family Agency Act 2013.

subjects and could lead to material and non-material damage. Thus, the severity of the risk is also high.

ii. Nature, Scope, Context and Purposes of Tusla's processing

7.15 In considering the appropriate level of security, regard must also be had to the nature, scope, context and purposes of Tusla's processing of personal data. As outlined above, the nature of Tusla's processing of personal data is inherently sensitive. Its scope is extensive in circumstances where it has State-wide responsibility for improving wellbeing and outcomes for children. The context of Tusla's processing is particularly relevant because it can occur parallel to adversarial disputes, such as in the area of family law or within its own appeals procedures. The purpose of Tusla's processing of personal data includes the safeguarding of children. Thus, the nature, scope, context and purposes of Tusla's processing of personal data require a high level of security.

7.16 Tusla confirmed that at the time of the breaches 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 breaches[4]. Despite this omission, for the purposes of this Decision, in considering the appropriateness of the technical and organisational measures that Tusla had in place at the time of the breaches, regard must be had to the high risk that Tusla's processing presented to the rights and freedoms of natural persons, and the sensitive and extensive nature, scope, context and purposes of the processing.

iii. Security measures implemented by Tusla

7.17 The Authorised Officers wrote to Tusla on 14th February 2020 asking it to provide specific information regarding what measures it had in place to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR in terms of:

1) An assessment of the risks of varying likelihood and severity associated with the forms of data processing at issue in the breaches;
2) Appropriate technical and organisational measures to counter those risks;
3) Capability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
4) Processes for regular testing, assessment and evaluating the effectiveness of the technical and organisation measures for ensuring the security of the processing.

7.18 Tusla responded to this letter on 21st February 2020 and stated that it had a number of technical measures in place at the time of the breaches to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

[4] Submissions dated 21st February 2020 at page 4.

These measures are set out in the document titled, '*Tusla ICT Technical Contols*', dated 5th Febraury 2020, which was appended to the letter. As decision-maker, I have considered the contents of this document. The document 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.

7.19 Tusla also provided the Authorised Officers with the document titled, *'Tusla's submissions on DPC Inquiry initiated in December 2018, Ref IN 18-11-000004'*, dated 13th February 2020. As decision-maker, I have considered the contents of this document. The document outlines, inter alia, the data protection training provided by Tusla to its staff. The training included: online mandatory GDPR training, which had an 85% completion rate as of 30th November 2018; specialist training for members of Tusla's DPU team; GDPR resources and guidance on Tusla's intranet; the Tusla newscast, a communications channel which was used to inform employees of key GDPR messages, and a list of newscasts between 12th February 2018 and 5th February 2019. Tusla's submissions dated 21st January 2020 contain details of three further newscasts issued between 3rd April 2019 and 31st May 2019. The resources included on Tusla's intranet include: policies, record of processing activities, Data Protection Impact Assessments, Vendor Privacy Assessments, Privacy Notices, Websites, Data Processors, Encrypted Email Functionality, Data Sharing with Other Public Bodies, Data Breaches, Data Subject Records Requests, Paper Based Records v Electronic Based Records, and Fax Machine Usage.

7.20 During the course of the Inquiry, Tusla also provided the document titled, "*Policy & Procedures for Responding to Allegations of Child Abuse & Neglect",* dated September 2014. This document sets out procedures for reports of allegations against alleged abusers, providing that alleged abusers have the right to copies of certain documents and further stipulating that *"If there is information in the relevant documents which relates to third parties, that may be redacted on the grounds of data protection."*[5]

iv. The appropriate level of security

7.21 For the reasons outlined below, I find that Tusla failed to implement appropriate organisational measures to ensure a level of security appropriate to the risk. In coming to this finding, I have had due regard to the risk presented by Tusla's processing to the rights and freedoms of natural persons; and the nature, scope, context and purpose of that

[5] At page 13.

processing; and the security measures that Tusla had implemented at the time of the beaches. I have also considered the state of the art and the costs of implementation with regard to measures that ought to have been implemented. The measures identified below are not to be interpreted as a comprehensive list of measures for Tusla's compliance with its obligation to implement appropriate organisational measures going forward. Rather, there is an ongoing obligation on Tusla to continually evaluate 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.

7.22 Tusla did not implement staff training that was specific to the redaction of documents shared with third parties. As outlined above, Tusla had implemented online mandatory GDPR training for its staff at the time of the breaches. It also implemented specialist training for members of Tusla's Data Protection Unit (DPU) team. However, the Inquiry found no evidence that any of the training incorporated instruction on how to comprehensively ensure that documents are properly redacted by relevant staff. In light of the high risk to the rights and freedoms of individuals from Tusla's sharing of documents with third parties, the organisational measures that Tusla was obliged to implement included specific training for redacting sensitive documents, to include scenario based training.

7.23 Tusla did not implement a formal written policy or rules for the redaction of documents. As outlined above, the Inquiry considered a range of data protection related policies that Tusla had in place at the time of the breaches, including the document titled, "*Policy & Procedures for Responding to Allegations of Child Abuse & Neglect"*. However, there is no evidence of any policy setting out specific rules or procedures for the redaction of documents before they are shared with third parties. In light of the scope of Tusla's processing of personal data, including the sharing of personal data with third parties, it was obliged to implement such a policy or rules. In the circumstances, such rules or policy should provide for a review and sign-off by a second member of Tusla's staff after redaction and before sharing with a third party in respect of sensitive documents.

7.24 Tusla did not implement any testing to evaluate the effectiveness of its redaction. The Inquiry found no evidence of any on-going oversight by management to ensure the effectiveness of Tusla's redaction of documents. It is noted that when the breaches came to light, Tusla was able to review the documents that were shared in some instances. However, Tusla presented no records of generalised testing of redacted documents to ensure its effectiveness. Such testing could take the form of managerial review of documents that are being shared or simulated redaction exercises for staff who are responsible for redaction. In light of the risk presented to the rights and freedoms of individuals by unauthorised disclosures, Tusla was obliged to implement organisational measures for the regular testing of the effectiveness of its redaction.

7.25 I have had regard to the cost of implementing the organisational measures identified in this part. I find that the staff training, formal written policy or rules, and the testing and managerial oversight would not impose a disproportionate cost on Tusla with regard to

their obligation to implement a level of security appropriate to the risk presented. I have also considered the state of the art software that is available on the market to assist with redaction. I note Tusla's submission that standard redaction software is currently used by it where possible. Such software tends to present both risks and opportunities regarding the security of personal data. Therefore, I consider that it is a matter for Tusla to consider the extent to which software would assist with its redaction responsibilities in the circumstances going forward. I further note that enhancements to Tusla's Case Management systems will allow files for redaction to go into a controlled workflow system for approval.

v. Finding

7.26 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 processing of personal data. The measures that ought to have been implemented include staff training specific to redaction, formal written policy or rules covering the redaction of documents, and testing and managerial oversight to evaluate the effectiveness of redaction.

B. Data Breach Notification

7.27 Tusla became aware of the third breach on 23rd May 2019. It notified the DPC of the breach on 28th May 2019 at 17:41pm by completing the data breach web form (Breach Notification BN-19-5-486). Tusla's reason for not notifying the DPC of the breach within 72 hours is that its own data protection unit was notified of the breach briefly by phone on 23rd May 2019, but the online form was not completed until late Friday evening (24th May 2019).

i. Analysis

7.28 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.'*

7.29 Regulation No 1182/71[6] determines the general rules applicable to periods, dates and time limits in EU Law and applies to the GDPR. Pursuant to Article 3(4) of the Regulation, the 72 hour period provided for in Article 33(1) of the GDPR includes Saturdays and Sundays. Tusla has not specified the exact time that the incident was detected on 23rd May 2019. However, it is clear that the 72 hour period expired some time on Sunday 26th May 2019.

7.30 The third breach created a risk to the rights and freedoms of the data subjects. The breach concerned the disclosure of the [redacted] In some circumstances, the disclosure of contact details and addresses might not be likely to result in a risk to the rights and freedoms of data subjects. However, regard must be had to the particular circumstances of the breach. The location of children in care may be highly sensitive in some circumstances. As noted by the Article 29 Working Party, *'if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and the child.'*[7] This is also the case [redacted] I have also had regard to the fact that one of the [redacted] and a vulnerable person. I find that this personal data breach had the potential to have an adverse effect on the data subjects and created a risk to their rights and freedoms. 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.

7.31 Tusla's failure to notify until 28th May 2019 constitutes an undue delay. There are no circumstances regarding this breach that justify Tusla's failure to notify the DPC within 72 hours of becoming aware of the breach. Tusla's reason for not notifying the DPC of the breach within 72 hours does not explain the delay. It states that the form was completed late on the Friday evening after becoming aware of the breach. This was the day after Tusla became aware of the breach, and well within the 72 hour period. There is no explanation for why the form was not submitted until the following Tuesday in circumstances where it had been completed four days earlier. I find that the delay of the notification was not justifiable in the circumstances.

ii. Finding

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

[6] Regulation (EEC, Euratom) No 1182/71 of the Council, of June 3 1971, determining the rules applicable to periods, dates and time limits.
[7] Article 29 Working Party, Guidelines on Personal Data breach notification under Regulation 2016/679, Adopted 6 February 2018, at page 24.

8. Corrective Measures

8.1 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 measures set out in Article 58(2):

a) Article 58(2)(b) - the issue of a reprimand to a Tusla in respect of its infringements of Articles 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 infringement of Article 32(1) of the GDPR.

A. Reprimand

8.2 I issue Tusla with reprimands under Article 58(2)(b) of the GDPR in respect of the infringements of Articles 32(1) and 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 processing of personal data, as required by Article 32(1), and failed to notify the DPC of the third breach without undue delay, as is required by Article 33(1) of the GDPR.

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

8.3 In accordance with Article 58(2)(d) of the GDPR, I order Tusla to bring its processing operations into compliance with Article 32(1) of the GDPR by implementing appropriate organisational measures to ensure a level of security appropriate to the risk caused by its processing of personal data. Tusla should perform a risk assessment to inform the measures that it must implement. However the manner of implementation of compliance is a matter for Tusla to decide.

8.4 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. I accept that the 2 month deadline proposed in the Draft Decision must be revised, in particular in light of Tusla's submissions on the challenges presented to it by the current COVID-19 crisis. I have also had regard to Tusla's detailed action plan, which was appended to the submissions. As a result, I order Tusla to bring its processing operations into compliance with Article 32(1) of the GDPR by **2nd November 2020**. [redacted]

In normal circumstances and were it not for the current pandemic, the timeframe for compliance, as indicated, would have been 2 months.

C. Administrative Fine

8.5 In addition the corrective powers under Article 58(2)(b) and (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

8.6 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.'

8.7 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;

8.8 I find that the infringement of Article 32(1) has a high degree of seriousness in terms of its nature, gravity and duration. Regarding the nature of the infringement, I have had regard to 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). Nonetheless, I find that the infringement is serious in nature due to the breadth of its reach across Tusla's processing. Tusla's failure to implement the appropriate organisational measures fundamentally undermined the security of a wide scope of its processing. In the specific circumstances where its functions require it to disclose personal data to third parties, redaction is essential to Tusla's general security of processing of personal data. Therefore, I consider the nature of the infringement of Article 32(1) in this case to be serious.

8.9 Regarding the gravity of the infringement, I have had regard to the fact that the infringement resulted in the three data breaches outlined in the Inquiry. It is not the case that this was a simple infringement of Article 32(1) without any resulting data breaches. There were a number of data subjects concerned in each breach and the loss of control over their data is significant in each case. Furthermore, the letters written by the [redacted] appended to the Final Inquiry Report at D.3.d, illustrate the high level of damage suffered by those [redacted] I have had regard to the varying impact that the breaches are likely to have had on the affected data subjects, and I note Tusla's submission that the first and third personal data breaches did not pose the same level of harm or impact. The fact that multiple data subjects were affected across three separate breaches illustrates the seriousness of the infringement and that the infringement is systemic.

8.10 Regarding the duration of the infringement, it is significant that the breaches occurred between 14th November 2018 and 14th March 2019. In the circumstances, it is clear that the infringement of Article 32(1) commenced at the enactment of the GDPR in May 2018. In those circumstances, the duration of the infringement is over 9 months in length. I consider that this duration adds to the seriousness of the infringement.

8.11 I find the nature, gravity and duration of the infringement of Article 33(1) is also serious. In particular, the fact that the recipient of the data used it to [redacted] contributes to the seriousness of Tusla's failure to notify the DPC without undue delay. Furthermore, the duration of the infringement is significant in circumstances where the notification should have been made within 72 hours and was 2 days late.

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

8.12 I find that Tusla's infringements were unintentional, but that they were negligent in character. Tusla was negligent in omitting to carry out a risk assessment to assess the risks of varying likelihood and severity associated with the forms of data processing at issue in the breaches and in failing to implement a level of security appropriate to that risk. Tusla was also negligent is failing to notify the DPC of the third breach without undue delay.

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

8.13 Tusla took action in respect of all three of the data breaches to mitigate the damage suffered by the data subjects. This action included seeking that the data disclosed be deleted by the recipients, planning for future communications in the case of the first breach, advising the recipients not to contact the data subjects directly, and liaising with Gardai and the local council concerning security, alternative housing, and school supports regarding the second breach.

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;***

8.14 As outlined in part 7(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.

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

8.15 There are no relevant previous infringements by Tusla.

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

8.16 Tusla cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its submissions on 21st January 2020 and 21st February 2020, Tusla outlined measures that it is adopting to mitigate against the breaches happening again. In its Detailed Action Plan, dated 31st March 2020, Tusla sets out the detailed project plans and timelines for implementation, which are illustrative of its continued efforts to address the infringements.

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

8.17 As an aggravating factor, I find that the categories of personal data affected by the infringement are particularly sensitive. Tulsa processes a significant amount of special category personal data and other personal data that is particularly sensitive. Some of this data may be disclosed to third parties in some circumstances. It is clear that redaction is essential to Tusla to ensure that special category data and other sensitive personal data is not inappropriately disclosed. Thus, Tusla's failure to implement appropriate organisational measures to ensure comprehensive redaction affects particularly sensitive categories of personal data. Furthermore, as is evident from the breaches, the dissemination of such unredacted personal data can cause immediate damage and distress to data subjects. Regarding the infringement of Article 33(1), Tusla's failure to notify the DPC without undue delay is aggravated by the fact that the personal data disclosed concerned the [redacted] and the [redacted] personal data that has the potential to be particularly sensitive in the circumstances.

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;***

8.18 The infringement became known to the DPC because Tusla notified the DPC of all three breaches. The second breach was also the subject of a complaint from one of the data subjects. 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 third 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;***

8.19 Not applicable.

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

8.20 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.***

8.21 I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

8.22 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 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 GDPR.

ii. Calculating the Administrative Fine

8.23 The Draft Decision set out a proposed range for the administrative fine, 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 made submissions to the effect that the administrative fine should be at the minimum of the range proposed in the Draft Decision based on a number of factors[8]. This Decision has had due regard to those factors in calculating the fine.

8.24 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.'*

[8] Tusla's Submission on the DPC's Draft Decision for Inquiry Ref: IN-19-10-01, at page 6.

8.25 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 Tusla's infringement of Article 32(1) the gravest infringement in the circumstances. Therefore, in calculating the administrative fine, I have had regard to this infringement only. The infringement of Article 33(1) is not considered aggravating for the purposes of calculating the fine.

8.26 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[9].

8.27 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.

8.28 The permitted range for this administrative fine is set out in Section 141(4) of the 2018 Act[10]. The fine shall not exceed €1,000,000 because Tusla is a public authority[11] that does not act as an 'undertaking' within the meaning of the Competition Act 2002[12]. 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 **€170,000** reflects the seriousness of this infringement and the aggravating factors. This figure is intended to reflect, in particular, the serious nature, gravity, and duration of the infringement and that some of the data subjects suffered a high level of damage, as set out in accordance with Articles 83(2)(a) above. It also reflects the fact that the categories

---

[9] 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.

[10] 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."

[11] 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.

[12] 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.

of personal data that were not protected by appropriate security measures are particularly sensitive, as considered in accordance Article 83(2)(g) detailed above.

8.29 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)(e), and 83(2)(f) of the GDPR mitigating. To take account for the unintentional character of the infringement, I have reduced the fine by **€15,000** in accordance with Article 83(2)(b). To account for the action taken by Tusla to mitigate the damage suffered by the data subjects, I have reduced the figure by **€40,000** in accordance with Article 83(2)(c). To account for the lack of relevant previous infringements by Tusla, I have reduced the figure by **€15,000** in accordance with Article 83(2)(e). To account for the cooperation that Tusla engaged with the DPC to remedy the infringement, including the Detailed Action Plan submitted on 2nd April 2020, I have reduced the figure by **€25,000** in accordance with Article 83(2)(f). Thus, the total figure for reducing the fine in light of the mitigating factor is **€95,000**.

8.30 Therefore, the final figure for the administrative fine is **€75,000**. I have considered this final figure in light of the requirement in Article 83(1) that administrative fines shall be "*effective, proportionate and dissuasive*". In considering the application of these principles, 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. I note that Tusla has an operational budget of over €750 million. In its submissions on the Draft Decision, Tusla emphasised the need for it to deploy its resources to the delivery of its vital services as the Child and Family Protection Agency for the State. However, as decision-maker for the Commission, I consider it important to strongly discourage the activity involved in this infringement. 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 **€75,000** meets the requirements of effectiveness, proportionality and dissuasiveness in respect of the infringement and data controller in issue. This amounts to **0.01%** of Tusla's operational budget, or **7.5%** of the cap available.

9. Right of Appeal

9.1 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