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-18-11-04

Commission Decision-Maker:

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

Date of Decision: 12th August 2020

Contents

1. Purpose of this Document 4
2. Background 4
3. Topics Arising in this Decision 6
4. Legal Regime Pertaining to the Inquiry and the Decision 8
5. Materials Considered 9
6. Data Controller 10
7. Personal Data 10
8. Analysis and Findings 11

A. Transmitting Personal Data on the NCCIS: Security of Processing 11

i. Assessing Risk 13
ii. Security Measures Implemented by Tusla 15
iii. The Appropriate Level of Security 15
iv. Finding 16

B. Transmitting Personal Data Internally by Email: Security of Processing 17

i. Assessing Risk 17
ii. Security Measures Implemented by Tusla 18
iii. The Appropriate Level of Security 19
iv. Finding 20

C. Transmitting Personal Data Externally: Security of Processing 20

i. Assessing Risk 20
ii. Security Measures Implemented by Tusla 21
iii. The Appropriate Level of Security 22
iv. Finding 24

D. Printing and Scanning: Security of Processing 24

i. Assessing Risk 24
ii. Security Measures Implemented by Tusla 25
iii. The Appropriate Level of Security 26
iv. Finding 26

E. Processes for Testing Security Measures: Security of Processing 26

i. Assessing Risk 27
ii. Security Measures Implemented by Tusla 28
iii. The Appropriate Level of Security 29
iv. Finding 30

F. Data Accuracy: Sharing Personal Data and Updating Tusla Records 30
i. Accuracy of Personal Data Disclosed to Third Parties 31
ii. Accuracy of Tusla's Internal Records 31
iii. Findings 32
G. Duty to Notify Personal Data Breaches 32
i. The Obligation to Notify Without Undue Delay 32
ii. The Breach Notifications 33
iii. Findings 39
H. Remaining Breach Notifications 39
9. Corrective Powers 40
A. Reprimand 41
B. Order to Bring Processing into Compliance 41
C. Administrative Fines 43
i. Decision to Impose Administrative Fines 43
ii. Linked Processing Operations 56
iii. Calculating the Administrative Fines 58
iv. Summary: Administrative Fines 62
10. Right of Appeal 62
Appendix: Personal Data Breaches Considered in the Inquiry 63

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 Inquiry Team of the DPC (**"the Inquiry Team")**. The Inquiry Team provided Tusla Child and Family Agency (**"Tusla"**) with the Draft Inquiry Report and the Final Inquiry Report. Tusla was provided with the Draft Decision on this Inquiry on 11th June 2020. 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 During the period of 25th May 2018 to 16th November 2018, Tusla notified the DPC of 71 personal data breaches (**"the breaches"**). On 6th December 2018, the Inquiry Team wrote to Tusla to notify it of the commencement of an own-volition inquiry pursuant to Section 110 of the 2018 Act in connection with the subject matter of the personal data breaches notified to the DPC. The decision to commence the Inquiry was taken following an examination of the specific details and context of the breach notifications and emails from Tusla providing additional information in relation to the breaches. The breaches were all in the nature of issues of unauthorised disclosure of, or access to, personal data processed by Tusla. The letter informed Tusla that the DPC would seek to establish a full set of facts so that it may assess whether or not Tusla has discharged its obligations in connection with the subject matter of the breaches and determine whether or not any provision(s) of the GDPR and/or the 2018 Act had been contravened by Tusla. The letter stated that the scope of the inquiry was to examine the practice and policies of Tusla in relation to training and awareness of staff and internal oversight by management of data protection principles in light of the obligations arising from the 2018 Act and the GDPR. It stated that the Inquiry would focus on data protection governance, training and awareness, records management (manual and electronic), security of personal data, data sharing, privacy impact assessments, and record of processing activities. The letter also set out a number of queries and sought particular information and documentation from Tusla.

2.2 On 13th February 2019, Tusla responded to the queries, including with the document titled, *"DPC Inquiry | Initiated in December 2018, Tusla Management Response, REF IN 18-11-000004, FINAL Version_v1.0, 13th February 2019",* and a listing and description of the materials that Tusla wished to submit, which were embedded within the listing. On 1st May

2019, Tusla submitted overviews of its ICT infrastructure, data processors, and social worker work flows to the Inquiry Team in advance of the DPC's pre-inspection meeting.

2.3 On 8th May 2019, the Inquiry Team conducted a pre-inspection meeting in Tusla's headquarters in the Brunel Building, Heuston South Quarter, Dublin 8. Tusla presented on its ICT infrastructure, data processors, and social worker work flows, and gave an overview of the strategic transformation in Tusla and actions that Tusla has progressed since the correspondence on 13th February 2019.

2.4 The Inquiry Team informed Tusla that it had prioritised 26 of the breaches and that it would commence on-site inspections at the locations where those breaches occurred. Inspections commenced on 5th June 2019 and occurred at the following locations: Carnegie Centre, Dublin 2; Naas, Co. Kildare; Community Services, Waterford; Airside Business Park, Swords, Co. Dublin; Newcastle Road, Galway; and Áras Sláinte, Cork.

2.5 On 17th January 2020, the Inquiry Team issued its Draft Inquiry Report to Tusla. It set out the Inquiry Team'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 Inquiry Team informed Tusla that it would consider any such submissions before proceeding to finalise the Inquiry Report. Tusla was given a 6 week deadline to provide submissions. On 11th February 2020, Tusla sought an extension to the deadline. The Inquiry Team refused this request in circumstances where the scale of the Inquiry had been taken into account when providing the original deadline.

2.6 Tusla made submissions on the Draft Inquiry Report on 28th February 2020. Those submissions included a proposed action plan to address *"systemic data protection issues"*. The submissions clarified inconsistent answers given to the DPC regarding monitoring access to the National Child Care Information System (**"NCCIS"**) and audit reports generated for this purpose. Tusla clarified that an NCCIS Security Audit Report was generated, but it was just not done in all areas or monitored nationally. Tusla also made submissions regarding, amongst other things, the ongoing risk analysis to identify threats and vulnerabilities to ICT services that it has undertaken since 2017; the reliance on HSE policies; the third party service provider in breach N-18-11-74; a new process for the automatic population of addresses; and Tusla's double authentication control for accessing NCCIS.

2.7 The Inquiry Team analysed the content of the submissions and amended the Draft Inquiry Report. On 4th March 2020, the Inquiry Team wrote to Tusla seeking further submissions regarding the measures 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) GDPR. Tusla responded on 19th March 2020 with submissions which included an overview of its submissions to date and the document titled, *"Organisational Risk Management Policy and Procedure"*, dated July 2016. In this letter, Tusla also sought clarifications on what information and / or guidance was provided to Tusla's staff members prior to questions being posed by the DPC investigators; the basis by which submission deadlines for the Inquiry were set; whether the Inquiry had transitioned into an Investigation pursuant to Section 137 of the 2018 Act; and the procedures for the publication of information.

2.8 The Inquiry Team responded on 20th March 2020. This letter clarified to Tusla that the oral submissions made by Tusla staff during the inspections were preceded by a clear explanation from the DPC that the information given may form part of the Inquiry Report. The letter also detailed how each inspection commenced with a clear introduction from the Inquiry Team explaining that the inspection was a fact gathering exercise as part of the Inquiry. The letter also reiterated that the process remained an Inquiry for the purposes of Section 110 of the 2018 Act, as notified to Tusla in the commencement letters and as referenced subsequently throughout the process, and had not transitioned into an Investigation under Chapter 5 of Part 6 of the 2018 Act. The letter also set out further information as to how deadlines for the Inquiry were set and regarding the publication of information.

2.9 In Tusla's letter dated 19th March 2020, Tusla also outlined that it had some concerns *"regarding certain potential factual inaccuracies which were recorded in the Draft Inquiry Report as a result of [the] site visits"*. These inaccuracies relate to information provided by Tusla staff to the Inquiry Team on the day of the inspections. Tusla's notes and clarifications on the Draft Inquiry Report, made in its submissions dated 28th February 2020, were analysed by the Inquiry Team and incorporated into the Final Inquiry Report as deemed appropriate by the Inquiry Team. I have also had regard those notes and clarifications for the purposes of this Decision. While inspections are a useful tool in gathering information relevant to an inquiry and may supplement the information obtained through written submissions and other means, they can result in inconsistent submissions as a result of submissions being made by various different sources within an organisation. Having regard to the nature of the issues raised in Tusla's submissions on the Draft Inquiry Report, and the fact that those submissions were made after Tusla was provided an opportunity to consider the Draft Inquiry Report in full, I accept that Tusla's submissions therein reflect the accurate position at the time of the personal data breaches. In this regard, I accept that an NCCIS Security Audit Report was a matter of local responsibility at the time of the breaches but that the reports were not generated in all areas or monitored nationally; that Tusla undertook the risk assessments and DPIAs in respect of the NCCIS as submitted; that *"reduced admin"* security roles on the NCCIS were based at local Area level, below regional level; that not all staff have access to the full national database on the NCCIS; that all of Tusla's USBs and laptops were encrypted by default; that the relevant ICT policies were assessed in 2018; and that staff sign an acceptable user form on setup of NCCIS.

2.10 On 3rd April 2020, the Inquiry Team 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 11th June 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 8th July 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. Topics Arising in this Decision

3.1 This Decision considers a broad range of Tusla's processing operations. The nature of the notified breaches are diverse and the context in which they occurred is equally broad. This Decision makes findings as to whether infringements of the GDPR and/or the 2018 Act have

occurred or are occurring considering all of the information obtained in the Inquiry. This includes, but is not limited to, the 71 breach notifications and the associated correspondence.

3.2 The findings in this Decision are also diverse. However, they can be divided into three thematic topics:

(i) Security of Processing,
(ii) Personal Data Accuracy, and
(iii) Notifications of Personal Data Breaches.

3.3 Some of the notifications to the DPC concern personal data breaches that occurred before the GDPR entered into force and before the 2018 Act commenced. Pursuant to Article 99 of the GDPR, the Regulation entered into force on 25th May 2018, which was also the specified date of applicability. The relevant provisions of the 2018 Act also commenced on that date[1] and that Act does not have retrospective effect[2]. Any information relating to those breaches is not probative as to whether Tusla has infringed provisions of the GDPR or the 2018 Act and the scope of the Inquiry concerns whether or not any provision(s) of the GDPR and/or the 2018 Act had been contravened by Tusla. Therefore, the following breaches are not considered for the purposes of this Decision:

Relevant Personal Data Breach Notifications: BN-18-8-209, BN-18-10-194, BN-18-6-41, BN-18-6-252, BN-18-9-246, BN-18-7-479, BN-18-7-236, BN-18-11-209, BN-18-6-285, and BN-18-6-299.

3.4 Having considered the notified breaches, it is clear that the root cause of some of them was a failure to implement redaction. Another 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. That Decision concerned the risk of unauthorised disclosure of personal data arising from a failure to implement appropriate redaction in the documents subject to Tusla's redaction operations. Decision IN-19-10-1 was made on foot of an Inquiry that was conducted by the DPC in relation to personal data breaches that occurred between 14th November 2018 and 14th March 2019. The finding of an infringement of Article 32(1) in Decision IN-19-10-1 concerned a period beginning at the coming into force of the GDPR until the date of the personal data breaches considered. Therefore, it concerns the same time period under consideration in this Decision. As the DPC has already considered the appropriateness of the technical and organisational measures implemented by Tusla regarding its redaction processes during this period, it follows that it is not necessary for this Decision to make findings regarding the security measures implemented regarding Tusla's redaction processing operations. Therefore, the following notified

[1] S.I. No. 174/2018 - Data Protection Act 2018 (Commencement) Order 2018.

[2] The presumption against retrospection was considered in Minister for Social, Community and Family Affairs v Scanlan [2001] 1 IR 64.

personal data breaches are not considered in this Decision, save where relevant to considering Tusla's compliance with the obligation to notify the DPC of personal data breaches without undue delay under Article 33(1):

Relevant Personal Data Breach Notifications: BN-18-9-400, BN-18-6-379, BN-18-9-249, and BN-18-9-480.

3.5 BN-18-9-400 and BN-18-9-480, the latter of which was also subject of a complaint with the Data Protection Commission, concern personal data breaches that occurred in relation to freedom of information requests concerning Tusla. These personal data breaches illustrate the importance of redaction in Tusla's freedom of information request procedures, not only to comply with its data protection obligations, but also to comply with its obligations pursuant to Section 37 of the Freedom of Information Act 2014. Decision IN-19-10-1 ordered Tusla to bring its redaction processing operations into compliance with Article 32(1) of the GDPR. As outlined in that decision, the measures that Tusla is obliged to implement pursuant to Article 32(1) of the GDPR regarding its redaction processes must be informed by a risk assessment.

3.6 Another Decision of the DPC (Decision IN-19-12-8, dated 21st May 2020), found that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate organisational measures in relation to the processing operation subject to that Decision. That processing operation concerned Tusla's issuing of safeguarding letters to third parties. That Decision considered the risk 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. It appears that Tusla's safeguarding letter processing operation may have been relevant to BN-18-6-299. However, in any event, as outlined above, this breach notification is not relevant for the purposes of this Decision as it relates to the period before the GDPR and the 2018 Act entered into force and were commenced respectively. I am satisfied that the remainder of the breach notifications are relevant for the purposes of this Decision and the information contained therein is considered accordingly.

4. Legal Regime Pertaining to the Inquiry and the 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. The Inquiry was commenced pursuant to Section 110 of the 2018 Act. Section 110(1) of the 2018 Act provides that the Commission may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the Commission may, for the purposes of

Section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding Section 135 of the 2018 Act) to be exercised.

4.2 In terms of the decision-making stage, which is set out under Section 111 of the 2018 Act, this provides that the Commission must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Inquiry Team.

5. Materials Considered

5.1 The Inquiry Team delivered the final Inquiry Report to me on 3rd April 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-18-11-04;
ii. The 71 Personal Data Breach Notifications submitted to the DPC and their related email correspondence;
iii. Letter of Notice of the Commencement of the Inquiry, dated 6th December 2018;
iv. Tusla's letter responding to the Commencement Letter, dated 13th February 2019;
v. Tusla's management response document, titled *"DPC Inquiry | Initiated in December 2018 Tusla Management Response"* and dated 13th February 2019;
vi. Tusla's *"Appendices"* document that accompanied the management response, dated 13th February 2019;
vii. Tusla's submitted *"Master breach listing"*, V0.4;
viii. NCCIS Data Migration & Quality Management Approach Document, V2.1, dated 4th October 2017;
ix. Summary paper on status of legacy systems migrated to NCCIS, dated January 2019;
x. Job specification, *"Job Specification Social Care Worker Special Care Job"*, submitted by Tusla on 13th February 2019;
xi. Tusla newscasts submitted to the DPC on 13th February 2019;
xii. Tusla's powerpoint extract from a SMT briefing, dated 23rd January 2019,
xiii. Tusla's Privacy Policy, May 2018
xiv. Tusla's Template Privacy Statement for Signage in Public / Reception Areas, submitted 13th February 2019;
xv. Tusla's Template Privacy Statement for Client & Employee Facing Forms, submitted 13th February 2019;
xvi. Tusla's CCTV Privacy Notice and CCTV Privacy Poster, submitted 13th February 2019;
xvii. Tusla's Data Privacy Notice and Privacy Notice Poster, submitted 13th February 2019;
xviii. Tusla's sample GDPR Induction Slides, dated 7th December 2018;
xix. Tusla's Freedom of Information Training Materials, submitted 13th February 2019;

xx. Policy and Procedure on Handling Freedom of Information Requests - FOI Act 2014, dated 20th January 2017;
xxi. Tusla's Freedom of Information catalogue of templates and guidance notes, submitted 13th February 2019;
xxii. Correspondence from Tusla's interim data protection officer and the DPC, dated 1st May 2019;
xxiii. Tusla's *"Tusla ICT Responses to DPC Letter Dated 01-04-2019"*;
xxiv. Tusla's document providing an overview of data processors that Tusla engages and what services they provide, submitted 1st May 2019;
xxv. Tusla's document providing an overview of an overview of how the Social Workers are engaging with personal data and their workflows, dated 1st May 2019;
xxvi. Tusla's proposed agenda for the meeting with the Inquiry Team on 8th May 2019; submitted 1st May 2019;
xxvii. Tusla's *"Presentation to the Data Protection Commission"* document, v1.0, dated 8th May 2019;
xxviii. The breach locations provided in appendix 5 to the Inquiry Report;
xxix. Tusla's Information Classification and Handling Policy, Revision 1.0;
xxx. Tusla's *"Protocol on Sending Child Protection Reports to Professionals in respect Child Protections Conferences on multiple children"*;
xxxi. Tusla's submissions on the Draft Inquiry Report, dated 28th February 2020;
xxxii. Correspondence between Tusla's data protection officer and the DPC dated 19th Match 2020;
xxxiii. Tusla's Organisational Risk Management Policy and Procedure, Rev 2.0, dated July 2018;
xxxiv. Tusla's Submission on the DPC's Draft Decision for Inquiry Ref: IN-18-11-04, Final v 1.0, submitted 8th July 2020; and
xxxv. All relevant correspondence between Tusla and the DPC.

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 breaches notified to the DPC and considered in this Decision concern personal data, save where otherwise specified below.

8. Analysis and Findings

8.1 Throughout the Inquiry, Tusla submitted details regarding a strategic transformation in place within the organisation and outlined a significant number of initiatives and deliverables underway to improve data protection practices and awareness. This Decision makes findings as to whether infringements of the GDPR and/or the 2018 Act have occurred by reference to the period under consideration in this Decision. 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 notified personal data breaches. However, it is acknowledged that some of the findings in this Decision may have since been addressed by Tusla or may be in the process of being addressed.

8.2 As outlined above, the Inquiry was commenced on an own volition basis in connection with the subject matter of the personal data breaches notified to the DPC. The information obtained in the breach notifications must be considered alongside all of the information obtained in the Inquiry. However, it does not necessarily follow from a controller's notification of a personal data breach that the breach was caused by an infringement of the GDPR or the 2018 Act. A controller's obligation to notify under Article 33(1) applies to all personal data breaches (unless unlikely to result in a risk to the rights and freedoms of natural persons) and is not dependent on the existence of an underlying infringement of the GDPR or the 2018 Act.

A. Transmitting Personal Data on the NCCIS: Security of Processing

Relevant Personal Data Breach Notification: BN-18-11-166.

8.3 The NCCIS is the central system used by Tusla to record the case history of every child who is the subject of a child protection or welfare referral to a social work department. It is a case management solution that allows immediate access to information about vulnerable children nationally. The roll out of the NCCIS started in mid-2017 and completed on 9th July 2018.

8.4 Breach BN-18-11-166 relates to unauthorised access within the NCCIS by an individual who was authorised to access the system. The breach occurred on 5th September 2018 when a member of Tusla's staff accessed a file on the NCCIS without a legitimate reason for doing so. [redacted] and the breach came to Tusla's attention when a data subject discovered it and complained to Tusla.

8.5 Tusla maintained audit logs for both edit and read only system transactions on the NCCIS, which confirmed that the records had been accessed by the member of staff. In its breach notification, Tusla submitted that it would undertake an analysis of the access controls in the NCCIS to determine how the employee accessed the data and to prevent similar issues arising in the future.

8.6 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.

8.7 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."*

8.8 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. Tusla stated that a Data Protection Impact Assessment, including the risk assessment, was undertaken by Tusla in 2013 and a further DPIA commenced in 2019. The DPC has not been furnished with any risk assessments undertaken by Tusla in relation to processing on the NCCIS. Nonetheless, in order to assess whether there has been an infringement of Article 32(1) of the GDPR, this Decision must assess the risk presented by Tusla's processing of personal data through the NCCIS. The technical and organisational measures that Tusla was obliged to implement are informed by the extent of the risk presented by this processing of personal data.

8.9 Article 32(4) of the GDPR provides:

> *"The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."*

i. Assessing Risk

8.10 The internal transmission of personal data on the NCCIS is a processing operation undertaken by Tusla. BN-18-11-166 illustrates that the risks to the rights and freedoms of individuals presented by this processing of personal data includes the risk that individuals who are authorised to access the NCCIS may access personal data without a legitimate reason. The technical and organisational measures that controllers and processors are obliged to implement must be appropriate to this risk.

8.11 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."*

8.12 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 individuals who have access to the NCCIS using it for non-legitimate reasons and, second, the severity of that risk to the rights and freedoms of the data subjects.

8.13 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others[3] provides guidance as to the factors that should inform this risk assessment. In this case, the CJEU declared the Data Retention Directive 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 NCCIS.

8.14 The quantity of the personal data processed by Tusla on the NCCIS is vast. The NCCIS records the case history of every child who is the subject of a child protection or welfare referral to a social work department. The personal data stored includes demographic and basic referral data, as well as case notes, forms, and assessment information. Furthermore, Tusla submitted that it retains certain personal data on the NCCIS in perpetuity. The NCCIS has been implemented nationally and covers all 17 areas within Tusla's jurisdiction. Therefore, the NCCIS processes personal data from all over the State. Tusla estimates that it received 6,000 referrals in 2019. Furthermore, there is likely to be

[3] 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).

a significant amount of personal data stored in respect of each child because the NCCIS is used to record personal data from first contact and assessment through to case closure.

8.15 The nature of the personal data processed on the NCCIS is highly sensitive. Tusla's functions include the provision of child welfare and protection services; domestic, sexual and gender-based violence services; and services related to the psychological welfare of children. Therefore, the personal data stored by Tusla on the NCCIS is likely to be highly sensitive in many instances, and will include special category personal data in some instances. Unauthorised access to or disclosure of this type of personal data has an inherent capacity to seriously infringe the rights and freedoms of data subjects.

8.16 The risk of unlawful access to the personal data is moderate. This risk is aggravated by the large number of individuals who have access to the NCCIS. Tusla's social workers and administrative staff require access to NCCIS across all business units. There are 1,800 social workers alone. Furthermore, it is clear that temporary staff and contractors also access the NCCIS. However, the risk is mitigated by the control that Tusla has over who those who can access the system. The NCISS is not accessible to the public and Tusla is in a position of control over employees and contractors with respect to their use of the NCCIS.

8.17 In assessing risk, regard must also be had to the scope, context and purposes of Tusla's processing of personal data on the NCCIS. The scope of processing is broad because it is used to record personal data for children in the State from first contact and assessment through to case closure and the personal data processed concerns a broad range of Tusla's functions concerning child welfare and family support services. The processing initiates in the context of child protection or welfare referrals. This context is relevant to assessing the risks to the rights and freedoms of data subjects because it indicates that data subjects may tend to be highly vulnerable. The purpose of the NCCIS is to provide a core national childcare management IT system to record the case history of children subject to child protection or welfare referrals. Tusla submitted on 13th February 2019 that "*The primary aim of the NCCIS is to improve the quality, safety, responsiveness and delivery of child services. NCCIS supports this aim by acting as a case management solution that allows immediate access to information about vulnerable children nationally."*[4] The system allows Tusla' staff to retrieve information necessary for their functions. Thus, the purpose of the system is not only to store information but it also makes that information immediately available to a significant number of Tusla's employees and contractors.

8.18 I find that Tusla's processing of personal data on the NCCIS poses a high risk to the rights and freedoms of natural persons. The risk includes the possibility that individuals who have access to the NCCIS might use it for non-legitimate reasons. The moderate likelihood of the risk must be balanced against the severity of that risk to the rights and freedoms of natural persons. The outcome of that balance is a high risk of material and non-

[4]Tusla Management Response, 13th February 2019, as page 16.

material damage to vulnerable data subjects due to the large-scale nature of the processing, including highly sensitive personal data, and the fact that particularly vulnerable data subjects are involved.

ii. Security Measures Implemented by Tusla

8.19 At the time of Breach BN-18-11-166, Tusla had implemented some technical and organisational measures that mitigate the risk of individuals, who have access to the NCCIS, using it for non-legitimate reasons. Users of the NCCIS were assigned to particular business units and their access to personal data was restricted accordingly. Access to basic referral data was unrestricted within the system, but access to assessments, plans, and case notes was restricted. Furthermore, by default, users could access detailed case information for their local area only.

8.20 Tusla required staff to sign an acceptable use form when being set up on the NCCIS. However, the system did not display a message at user logon warning the user that the system should only be used for specific legitimate reasons or that Tusla is monitoring the system for inappropriate access. The Inquiry Team noted that such logon messages are used by other public sector bodies. Furthermore, the Inquiry Team also found no evidence that the issue of inappropriate access is raised at staff induction for new staff. Tusla implemented mandatory GDPR training for staff in 2018. The Tusla Newscast, a communications channel made available to all staff, was used by Tusla to communicate key data protection messages to staff. However, the Inquiry Team found no evidence of training regarding the specific issue of inappropriate staff access to personal data.

8.21 Regarding Tusla's ability to identify unauthorised access to personal data within the NCCIS, Tusla maintained some audit trail functionality at the time of the breach. Tusla submitted to the Inquiry Team on 10th July 2019 that there is a NCCIS Security Audit Report that may be accessed by relevant staff. However, during the Inquiry Team's site inspection at Tusla headquarters on 24th July 2019, Tusla stated that no NCCIS Security Audit Report was generated. Tusla's submissions on the Draft Inquiry Report, dated 28th February 2020, clarifies that, at the time of the submissions, the operation of the existing draft policy on the Security Audit Report was a matter of local responsibility. This meant that there was no national oversight and that not all areas were operating the policy. Tusla is now implementing a process to monitor quarterly security audits.

iii. The Appropriate Level of Security

8.22 Having regard to the high risk to the rights and freedoms of natural persons presented by Tusla's internal transmission of personal data on the NCCIS, I find that an appropriate level of security must include a display message at every user logon informing users that the system should only be used for legitimate reasons and that Tusla is monitoring the system for inappropriate access. This significant measure is appropriate, in particular, because of the amount of personal data stored on the system, the large number of staff

and contractors who have access to it, and the risk of scenarios arising, such as in Breach BN-18-11-166, [redacted] to access personal data stored on the NCCIS. In light of the nature of Tusla's functions, an appropriate level of security must also include specific instruction to all staff at induction regarding the issue of inappropriate access to personal data encountered during the course of their employment. This should also be addressed in regular training provided to existing staff. In the absence of such a display message and staff instruction and training, Tusla failed to implement technical and organisational measures that were appropriate to the risk.

8.23 An appropriate level of security must also include regular national and local auditing of the access logs to the NCCIS in order to identify inappropriate usage and access. The situation in place at the time of BN-18-11-16, whereby there was no national oversight and not all areas were auditing the logs, does not meet the appropriate level of security. I note Tusla's submissions that it is currently developing a proactive protocol for identifying and managing unusual access patterns on the NCCIS, including a benchmark of what normal access looks like. I also note that Tusla is currently scoping the feasibility of adding a mandatory requirement to NCCIS, requiring users to record a business reason when accessing cases owned by other users, in line with the recommendations made by the DPC's Special Investigation Unit in 2017. I consider the implementation of this recommendation a matter for Tusla to consider, with regard to its obligation to implement an appropriate level of security, following the conclusion of its feasibility assessment.

8.24 I have had regard to the likely cost of implementing a display message at every user logon, staff instruction at induction and regular training regarding inappropriate access to personal data, and regular national and local auditing of the access logs. I find that implementing such measures 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 measures 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.

iv. Finding

8.25 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its internal transmission of personal data on the NCCIS. The measures that ought to have been implemented include a display message at every user logon, staff instruction at induction and regular training for existing staff regarding inappropriate access to personal data, and regular national and local auditing of the access logs. By failing to implement these measures, Tusla also infringed Article 32(4) of the GDPR in that Tusla failed to take steps to ensure that any natural person acting under their authority does not process personal data on the NCCIS except on instructions from Tusla.

B. Transmitting Personal Data Internally by Email: Security of Processing

Relevant Personal Data Breach Notifications: BN-18-8-146, BN-18-8-339, BN-18-6-534, BN-18-6-53, BN-18-6-227, BN-18-6-571, BN-18-7-266, BN-18-7-603, BN-18-8-236, and BN-18-8-316.

8.26 The notified personal data breaches illustrate how Tusla uses internal email, in addition to the NCCIS, to transmit the personal data of data subjects between staff. This creates the risk of an email being sent to the wrong recipient, resulting in an unauthorised disclosure of personal data. 10 of the notified personal data breaches occurred where a Tusla employee intended to email another Tusla employee, but instead emailed an employee of the HSE. Tusla's email system includes global address lists, which allow staff to select both Tusla and HSE email addresses. The availability of HSE emails on these lists contributed to the 10 personal data breaches. The technical and organisational measures that Tusla is obliged to implement in respect of this risk must be informed by a risk assessment.

i. Assessing Risk

8.27 The risk to the rights and freedoms of data subjects caused by internal Tusla emails being sent to the wrong email address and disclosing the personal data of data subjects 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. As outlined in Part 8(A)(i) of this Decision, this assessment involves a consideration of the quantity of the personal data processed, the nature of that personal data, the risk of unlawful access, and the scope, context and purposes of Tusla's processing of personal data.

8.28 There is a high likelihood of internal Tusla emails being sent to the wrong email address in circumstances where the global address lists include HSE addresses. Both organisations have a large number of employees. This aggravates the risk because of the large number of internal emails that are likely to be sent daily and the high likelihood of similar email addresses within the Tusla and HSE domains respectively. Furthermore, the global address lists can result in a single email being accidentally sent to multiple external HSE employees. BN-18-8-146 concerned a list of service users in the [redacted] process being sent to [redacted] employees of the HSE. This was intended to be an internal email to another Tusla employee. The fact that the 10 notified breaches occurred in such a short period of time further indicates the high likelihood of this risk. It is also significant that a single email can result in the disclosure of a large number of data subjects' personal data, as was the case in BN-18-6-534, where an email to a HSE email address inadvertently disclosed the personal data of 13 young people in care, 27 young people who had previously been in care, and 2 young people in care who are over 18 years of age.

8.29 The severity of the risk is moderate. A significant quantity of personal data is exchanged between Tusla staff by internal email. The 10 personal data breaches alone included the transmission of a list of service users in [redacted]; the personal data of a missing child; identity and contact details made in the context of a protected disclosure; minutes of a meeting, a foster care contract; names, dates of birth, and parents' names of service users; and details of a freedom of information request. As is clear from the personal data transmitted in the 10 personal data breaches, the nature of this personal data is highly sensitive in some instances, for example the identity of service users [redacted]. The severity of the risk to the rights and freedoms of natural persons is mitigated because individuals with HSE email addresses could be considered trusted recipients depending on the circumstances of a particular personal data breach. It is noted that in breaches BN-18-6-534, BN-18-6-53, BN-18-6-571, BN-18-7-266, BN-18-8-316 and BN-18-8-236 the relevant HSE employees confirmed that the emails had been deleted. However, depending on the nature of the personal data and the context of the processing, this will not always mitigate the risk to the rights and freedoms of the data subjects. For example, regarding the unauthorised disclosure regarding a protected disclosure in BN-18-6-227, it is not mitigating that the recipient of that personal data was the HSE. The disclosure of the identity of makers of protected disclosures has the potential to pose a severe risk to the rights and freedoms of the individual making the disclosure, regardless of the recipient, and is afforded specific protection by Section 16 of the Protected Disclosures Act 2014.

8.30 I find that Tusla's transmission of personal data by internal email between staff poses a moderate risk to the rights and freedoms of the data subjects. Although the likelihood of this risk is high in circumstances where the global address lists include external HSE email addresses and both organisations have a large number of employees, the high likelihood must be balanced against the moderate severity of the risk where individuals with HSE email addresses could be considered trusted recipients depending on the circumstances of a particular personal data breach.

ii. Security Measures Implemented by Tusla

8.31 The availability of HSE email addresses in the global address lists heightens the risk of internal Tusla emails being sent to HSE email accounts. The Inquiry discovered no evidence of technical measures implemented by Tusla to address this risk. Furthermore, on the date of the inspection at Airside Business Park, the Inquiry discovered no evidence of restrictions being implemented on access to global address lists.

8.32 At the time of the breaches, Tusla had implemented its *"Information Classification and Handling Policy"*, which came into effect on 25th May 2018. The policy does not require sensitive personal data transmitted by email to be protected by passwords in respect of any emails, regardless of their sensitivity. Such protection may be provided by a policy that requires sensitive personal data to be provided in an attachment to an email, with such attachments being password protected. The password is then communicated by some other means to the recipient. The *"Information Classification and Handling Policy"*

requires encryption for confidential and strictly confidential emails. Encryption generally renders emails unreadable until they reach their destination. This protects the contents of emails from the threat of interception as they travel from origin to destination. However, once they reach their destination, depending on the nature of the measures implemented, encryption may not restrict emails from being accessed by the recipient. Therefore, the *"Information Classification and Handling Policy"* does not address the risk of emails being sent to the wrong recipient.

iii. The Appropriate Level of Security

8.33 Having regard to the moderate risk to the rights and freedoms of natural persons presented by Tusla's transmission of personal data between staff by internal email, I find that an appropriate level of security must include a technical measure that specifically addresses the risk posed by HSE email addresses being included in the global address lists. In its submissions on the Draft Decision, Tusla outlined that it is in the process of migrating email users off the HSE email system to create a *"Tusla only"* email infrastructure[5]. I find that this measure, once completed, is sufficient with regard to the risk presented.

8.34 I find that an appropriate level of security must also include a policy that mandates password protection for sensitive personal data transmitted by email. As outlined above, Tusla's *"Information Classification and Handling Policy"* requires encryption in email for *"confidential"* and *"strictly confidential information"* in both internal and external email. However, it does not require sensitive personal data transmitted by email to be protected by passwords. Therefore, there is no protection against the risk of an unauthorised disclosure of personal data arising from an email being sent to the wrong recipient. I note Tusla's submission on the Draft Decision in which it outlined the need for Tusla staff to exchange information by email urgently in some instances, particularly in relation to urgent child protection incidents. The precise details of the policy mandating password protection, and any justifiable exceptions contained within that policy, must be informed by Tusla's risk assessment and its own functions. Therefore, when determining whether the appropriate level of security allows for certain exceptions to this policy, it is appropriate for Tusla to have regard to the need for its staff to urgently exchange information to protect the rights and freedoms of children in some instances.

8.35 I have had regard to the likely cost of implementing the technical and organisational measures outlined in this part. I find that implementing such measures would not impose a disproportionate cost on Tusla with regard to their obligation to implement a level of security appropriate to the risk presented. In particular, Tusla appears to already be in the the process of creating a *"Tusla only"* email infrastructure to address the risk of HSE email addresses being included in the global address lists. Furthermore, a policy requiring password protected attachments for sensitive personal data transmitted by email would not impose a cost on Tusla that is disproportionate to the risk to the rights and freedoms of data subjects. However, it should be noted that implementing such measures does not

[5] Tusla's submission on the DPC's Draft Decision, at pages 12 and 19.

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.

iv. Finding

8.36 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its transmission of personal data between staff by internal email. The measures that ought to have been implemented include a technical measure to address the availability of HSE email addresses on the global address lists, and a policy that requires sensitive personal data transmitted by email to be protected by passwords.

C. Transmitting Personal Data Externally: Security of Processing

Relevant Personal Data Breach Notifications: BN-18-8-476, BN-18-10-18, BN 18-11-74, BN-18-7-602, BN-18-7-303, BN-18-6-191,BN-18-6-549, BN-18-7-322, BN-18-8-454, BN-18-8-338, BN-18-6-250, BN-18-9-289, BN-18-11-158, BN-18-6-288, BN-18-6-411, BN-18-6-316, BN-18-8-297, BN-18-8-120, BN-18-8-244, BN-18-8-333, BN-18-9-156, BN-18-8-315, BN-18-8-519, BN-18-10-402, BN-18-9-57, BN-18-9-289, BN-18-10-439, and BN-18-11-75.

8.37 These notified personal data breaches illustrate that Tusla uses email and post to transmit personal data to external recipients, including service users. Tusla's functions also require it to issue certain types of letters and forms repeatedly to different external recipients. Tusla's staff have used previously drafted letters and forms that contain personal data as templates for those letters.

8.38 As is evident from the notified breaches, Tusla's transmission of personal data externally creates the risk of unauthorised disclosure of personal data in two ways. First, this risk manifests in correspondence being delivered to the wrong postal or email address. This risk is similar to that identified at part 8(B) above. However, it also includes the risk of unauthorised disclosures through post. Second, the risk manifests in personal data in prepopulated templates being inadvertently disclosed in subsequent letters. The technical and organisational measures that Tusla is obliged to implement must be appropriate to those risks.

i. Assessing Risk

8.39 The risk to the rights and freedoms of data subjects caused by address errors or template errors when transmitting personal data externally 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. As outlined in Part 8(A)(i) of this Decision, this assessment involves a consideration of the quantity of the personal data processed, the nature of that personal data, the risk of unlawful access, and the scope, context and purposes of Tusla's processing of personal data.

8.40 There is a high likelihood of address errors and template errors being made by Tusla when transmitting personal data externally. The risk of such errors occurring is high due to the number of staff and amount of correspondence that Tusla is required to issue. This risk is even greater for Tusla than other large organisations because, as is evident from the notified personal data breaches, in addition to standard correspondence, it is required to issue formal letters regarding results of fostering applications, acknowledgement letters regarding reports of concern about children, placement reports, and minutes from sensitive case conferences. The nature of Tusla's functions increases the amount of correspondence it issues through letters, emails, and forms. This creates a high risk of address and template errors resulting in unauthorised disclosures of personal data. The range of recipients that Tusla is required to correspond with also increases the risk.

8.41 The severity of the risk is also high. The personal data that Tusla transmits with external recipients is often highly sensitive. For example, correspondence concerning allegations of sexual abuse were subject of unauthorised disclosure through address based errors (BN-18-6-549). The quantity of personal data that could potentially be disclosed in a single data breach is also high, for example through the minutes of case conferences or reports being disclosed to the wrong recipient. In BN-18-7-303 the personal data of [redacted] in case conference minutes were the subject of an unauthorised disclosure. The unauthorised disclosure of sensitive and/or a high quantity of personal data has the inherent capacity to cause material and non-material damage to data subjects. The extent of the damage may, in many cases be difficult to assess, for example in BN-18-6-250, where sensitive personal data was disclosed to an unknown recipient due to a typographical error.

8.42 I find that there is a high risk to the rights and freedoms of natural persons caused by Tusla's transmission of personal data with external recipients. This risk manifests in emails or post being sent to the wrong address or in personal data being copied into correspondence from previous template letters and forms. Although the risk of address and template errors is acute in large organisations, it is crucial that Tusla implements appropriate technical and organisational measures to address this risk.

ii. Security Measures Implemented by Tusla

8.43 Some of the regional areas in Tusla had templates for commonly used letters and forms at the time of the breaches. During the inspection at Waterford/Wexford Community Services, the Inquiry Team noted that templates had been developed locally, despite the fact that the relevant template wasn't used in relation to breach BN-18-10-18. Fostering Departments in the Northwest of Ireland have also agreed common templates. However, such templates are not available in all of Tusla's regional areas. The lack of such templates contributed to a personal data breach in Dublin South Central (BN-18-8-476) and Dublin North East (BN-18-11-74). Furthermore, where templates did exist, they were implemented at the initiative of the local offices. There was no co-ordinated national approach to templates initiated by Tusla.

8.44 The implementation of blank templates for commonly used letters and forms in Waterford/Wexford Community Services and the fostering department in Northwest of Ireland reduces the risk of unauthorised disclosures of personal data by reducing the likelihood of staff relying on previously issued letters as templates for letters being sent to different recipients. However, some regional areas in Tusla used letters that contained previously issued names, addresses, and sensitive personal data as templates for subsequent letters issued to different recipients. Tusla's use of such templates is most concerning. During the inspection in Cork, the Inquiry Team noted that a Tusla shared drive contained template letters that contained the personal data from previously issued letters. Similarly, Breach BN-18-7-602 occurred in the Galway/Roscommon region due to the use of a template that contained the personal data of another data subject. The use of templates that contain personal data from previously issued letters poses a severe and unjustifiable risk to the rights and freedoms of the individual whose personal data is used in the template. An unauthorised disclosure of the data subject's personal data could potentially occur every time that a Tusla staff member views the template. Furthermore, there is a risk of errors, such as in BN-18-7-602, whereby personal data was not removed from templates and was sent to service users in new letters within the same region.

8.45 Regarding the risk of emails being sent to the wrong recipient, as noted at Part 8(B)(ii) above, Tusla had implemented its *"Information Classification and Handling Policy"* at the time of the time of the breaches. In respect of emails that are sent externally, encryption is also required for *"confidential information"* and *"strictly confidential information"*. However, as noted above, the policy does not require password protection for sensitive personal data transmitted by email.

8.46 Regarding the risk of post being sent to the wrong recipient, Tusla's *"Information Classification and Handling Policy"* requires *"confidential information"* and *"strictly confidential information"* to be scanned and sent by encrypted email if feasible. There is no requirement for such scanned documents to be password protected. Where email isn't feasible, the policy requires such letters to be sent by registered post or courier, and to be marked confidential. There is no provision in the policy for letters to be double-checked by a second member of Tusla staff where email is not feasible for sensitive letters. For example, in Breach BN-18-8-454 a letter containing sensitive personal data was sent to an incorrect address and opened in circumstances where there was no process in place for reviewing sensitive information being released.

iii. The Appropriate Level of Security

8.47 Having regard to the high risk to the rights and freedoms of natural persons presented by Tusla's external transmission of personal data, I find that an appropriate level of security must include co-ordinated national templates for commonly issued letters and forms. I note Tusla's submission that it proposes to*:*

"Establish an internal audit process to ensure templates are used correctly, e.g. blank templates are maintained and stored on file, blank templates are not overwritten with personal information, etc. and conduct internal audits on a regular basis"[6]

8.48 This proposal is not sufficient to address the high risk to the rights and freedoms of natural persons. In light of the high quantity of correspondence issued by Tusla, an audit process is not sufficient to address the risk of Tusla's staff relying on previously issued letters and copying and pasting information accordingly. To implement a level of security appropriate to the risk, the templates must be incorporated into web-based forms that automatically revert to empty when correspondence is issued. Tusla submitted that it currently has the ability to create such documents for the Child Abuse Substantiation Procedure module only[7]. I find that an appropriate level of security requires such templates for all commonly issued letters and forms that contain sensitive personal data. In addition, the use of templates containing personal data from previous letters must be prohibited.

8.49 As outlined above regarding Tusla's transmission of personal data internally by email, an appropriate level of security for that processing operation requires a policy mandating that sensitive personal data transmitted by email be password protected. This measure is also appropriate in relation to Tusla's transmission of personal data externally by email. As outlined above, any justifiable exceptions contained within that policy must be informed by Tusla's risk assessment and its own functions, which may have regard to the need for Tusla staff to urgently share personal data in some circumstances. However, the appropriate level of security must also include a policy that mandates a second review of letters containing sensitive personal data sent by post where it is not feasible to send that correspondence in a password protected form by email. Tusla's *"Information Classification and Handling Policy"* simply requires such letters to be sent by Registered Post or Courier and to be marked confidential. However, in light of the high quantity of sensitive personal data processed by Tusla, a second review, where password protection via email is not feasible, is appropriate.

8.50 I have had regard to the likely cost of implementing co-ordinated templates in web-based forms, and reviewing sensitive letters sent by post where sending the correspondence in a password protected manner via email is not feasible. I find that implementing such measures would not impose a disproportionate cost on Tusla with regard to their obligation to implement a level of security appropriate to the risk presented. It is acknowledged that the second review of all sensitive letters sent by post would require significant resources from Tusla. However, this can be mitigated by the requirement for correspondence with sensitive personal data to be sent in a password protected manner via email where feasible. However, it should be noted that implementing such measures 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.

[6] Tusla's Response to the DPC's Draft Inquiry Report (IN-18-11-04), dated 28th February 2020, at page 5.
[7] Ibid at page 6.

iv. Finding

8.51 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its external transmission of personal data. The measures that ought to have been implemented include co-ordinated templates for commonly issued letters, a policy mandating that sensitive personal data transmitted by email be password protected, web-based forms that automatically revert to empty when correspondence is issued, and an organisation-wide policy requiring the review of sensitive letters sent by post.

D. Printing and Scanning: Security of Processing

Relevant Personal Data Breach Notifications: BN-18-8-536, BN-18-6-584 and BN-18-8-184.

8.52 At the time of the personal data breaches, Tusla had not implemented a secure identification facility for printing and scanning across the entire organisation. In breach BN-18-8-536, a Tusla staff member scanned a document with special category personal data concerning vulnerable individuals. They manually entered the email address that they intended to deliver the scan to. However, instead of sending the scan to their own email address, they inadvertently sent it to an external third party. Breach BN-18-6-584 occurred where a Tusla contractor sent files to a Tusla printer. The secure ID printing facility did not engage and the files automatically printed. This resulted in the files being viewed by an employee of Tusla who was not authorised to view them. BN-18-8-184 occurred when a standard report form concerning [redacted] was collected from a Tusla printer along with Human Resources documents. The entire bundle of documents was inadvertently placed in the personnel file of a Tusla staff member. This error was discovered during a review of the personnel file. The technical and organisational measures that Tusla is obliged to implement must be appropriate to the risk to the rights and freedoms of data subjects posed by the unauthorised disclosure of personal data caused by Tusla's printing and scanning of documents.

i. Assessing Risk

8.53 The risk to the rights and freedoms of data subjects posed by the unauthorised disclosure of personal data caused by Tusla's printing and scanning of documents 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. As outlined in Part 8(A)(i) of this Decision, this assessment involves a consideration of quantity of the personal data processed, the nature of that personal data, the risk of unlawful access, and the scope, context and purposes of Tusla's processing of personal data.

8.54 The likelihood of an unauthorised disclosure of personal data occurring in relation to Tusla's printing and scanning of documents is moderate. It is noted that BN-18-8-536 occurred due to an error made by a member of staff when inputting their email address. Further, it appears from BN-18-6-584 that Secure ID printing was used in respect of some or all of Tusla's printers but that it failed to engage in this instance, potentially because a contractor was printing to the system. However, Tusla is likely to undertake a significant quantity of printing and scanning in light its functions and size. Therefore, in the absence of secure ID printing and scanning, the likelihood of an unauthorised disclosure is moderate.

8.55 The severity of the risk is high. Tusla's functions require it to frequently process highly sensitive personal data. Its printing and scanning can result in the unauthorised disclosure of special category data concerning vulnerable individuals as was the case in Breach BN-18-8-536. Regarding scanning, the severity of the risk is increased by the possibility of an unauthorised disclosure occurring with an external third party. This creates a high severity risk to the rights and freedoms of those data subjects. However, it is acknowledged that unauthorised disclosures from printing is more likely to relate to trusted recipients, i.e. Tusla staff.

8.56 I find that Tusla's printing and scanning operations pose a high risk to the rights and freedoms of the data subjects. The moderate likelihood of the risk must be balanced against the high severity of the risk, particularly in relation to scanning, whereby special category personal data concerning vulnerable individuals can be disclosed to external recipients. This balance results in an overall high risk to the rights and freedoms of the data subjects.

ii. Security Measures Implemented by Tusla

8.57 At the time of the breaches, Tusla had partially implemented secure print facilities. However, the secure printing did not engage when breach BN-18-6-584 occurred and the Inquiry Team noted that secure ID printing was not implemented across the organisation. Regarding BN-18-8-184, at the inspection at Dublin North East, Airside Business Park, the Inquiry Team noted that secure printing had not been made available at every Tusla location. Commonly available secure print facilities allow documents that are sent to a printer to be stored on it until the sender authenticates at the location of the printer with a badge or PIN. This facility can be made available to employees on a permanent basis and also to visitors or contractors temporarily.

8.58 At the time of Breach BN-18-8-536, Tusla had not implemented secure ID scanning. Similar to secure ID printing, this facility allows a token to be set up that ensures delivery to a unique address. This provides the option for an individual to opt to send the scans to themselves, without having to manually input their email address. This reduces the risk of errors from inputting email addresses manually.

iii. The Appropriate Level of Security

8.59 Having regard to the high risk to the rights and freedoms of natural persons presented by Tusla's printing and scanning operations, I find that an appropriate level of security must include fully implemented secure print facilities and secure scan facilities. I have had regard to the likely cost of implementing these technical measures. I find that implementing such measures would not impose a disproportionate cost on Tusla with regard to their obligation to implement a level of security appropriate to the risk presented. Secure print and scan facilities are commonly available and it appears that Tusla has already partially implemented the secure print facility. However, it should be noted that implementing such measures 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.

iv. Finding

8.60 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate technical measures to ensure a level of security appropriate to the risk presented by its printing and scanning operations. The measures that ought to have been implemented include fully organisation-wide secure print facilities and a secure scanning facility.

E. Processes for Testing Security Measures: Security of Processing

Relevant Personal Data Breach Notifications: BN-18-6-482, BN-18-7-471, BN-18-7-124, BN-18-10-115, BN-18-8-29 and BN-18-9-43.

8.61 Some of the notified personal data breaches occurred when Tusla staff ignored and/or failed to apply policies that Tusla had in place to provide for the security of the personal data being processed. BN-18-6-482 occurred where a service user [redacted] and viewed a forensic report therein. Tusla's *"Records Management Policy"*, Revision Date April 2018, was in place at the time, implementing a clean desk and clear screen policy[8] and also requiring that files containing personal data be kept locked in a filing cabinet when not being used. Tusla submitted that these policies were not adhered to, which resulted in the breach occurring. BN-18-7-471 occurred when Tusla posted a care plan [redacted] by ordinary post. When the letter arrived at [redacted], it was open and the contents had been removed from the envelope. It is not clear how or when the care plan was removed. Tusla's *"Information Classification and Handling Policy"*, revision 1.0, was in place at the time of the breach, which required such a letter to be issued by registered post. The failure to comply with this policy may have contributed to the personal data breach. BN-18-7-124 occurred when a [redacted] in the Tusla [redacted] lost hardcopy files [redacted]. The files contained the

[8] At page 13.

personal data of 150 data subjects, including personal data revealing racial or ethnic origin, religious or philosophical beliefs, and health data. Tusla's *"Records Management Policy"*, revision 4, was in place at the time of the breach and required documents to be stored securely when being transferred outside the office[9]. Furthermore, Tusla's *"Information Classification and Handling Policy"* required that the documents be circulated by encrypted email in this instance. Tusla submitted that the breach was caused by a failure to comply with this policy[10]. BN-18-10-115 occurred when a Tusla staff member lost a form containing a child's personal data when transporting it from [redacted] As outlined above, Tusla's *"Records Management Policy"*, revision 4, required documents to be stored securely when being transferred outside the office. This policy document is an organisational measure used to communicate to staff, amongst other things, the need for the secure transportation of documents. BN-18-8-29 and BN-18-9-43 both occurred when Tusla emailed documents to the correct intended recipient, but attached the incorrect documents, resulting in an unauthorised disclosure of personal data. Following these breaches, Tusla identified certain measures to reduce the risk of these errors occurring. Such measures could have been identified by Tusla prior to the breaches occurring through a process for testing the effectiveness of the existing measures that Tusla had in place.

8.62 The obligation to implement appropriate technical and organisational measures under Article 32(1) may include, if appropriate:

> *"a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*[11]

8.63 The measures provided for in Tusla's *"Records Management Policy"* and *"Information Classification and Handling Policy"* are only effective insofar as Tusla's staff apply them. The level of testing that Tusla was obliged to implement regarding the effectiveness of the measures must be informed by a risk analysis. The risk analysis must consider the risk to the rights and freedoms of data subjects caused by the non-implementation of the *"Records Management Policy"* or the *"Information Classification and Handling Policy"*.

i. Assessing Risk

8.64 The risk to the rights and freedoms of data subjects caused by the non-implementation of the *"Records Management Policy"* or the *"Information Classification and Handling Policy"* 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. As outlined in Part 8(A)(i) of this Decision, this assessment involves a consideration of quantity of the

[9] At page 15.

[10] Tusla submitted in its breach notification that: *"The documentation was issued by courier, however, the files were not stored securely by the individual who received the files in advance of the meeting. There was a failure to follow the requirements of the information handling and classification policy around confidential and restricted information i.e. that it be circulated by encrypted email if possible."*

[11] Article 32(1)(d) GDPR.

personal data processed, the nature of that personal data, the risk of unlawful access, and the scope, context and purposes of Tusla's processing of personal data.

8.65 The likelihood of staff failing to apply the provisions of the *"Records Management Policy"* or the *"Information Classification and Handling Policy"* is moderate. The measures are of general application and are dependent on implementation by most, if not all, staff. The clean desk and clear screen policies are applicable to all staff and the policies regarding the sending of certain correspondence by encryption or registered post are likely to be applicable to a large number of staff who are required to issue such correspondence. The policy regarding the secure storage of documents when being transferred outside the office is likely applicable to less staff who are required to transfer documents outside of the office. Furthermore, the nature of the policies require them to be engrained in staffs' daily functions as issues such as clear desks and screens, transmitting confidential information, and secure storage are likely to arise on daily basis for most staff. Therefore, the number of staff who are required to implement these policies, and the frequency with which they must be implemented, increases the risk that they may fail to be applied. However, the likelihood of the risk is mitigated by the practical nature of the policies, which some staff may consider to be intrinsic to handling the sensitive personal data processed by Tusla, regardless of the existence of the policies.

8.66 The severity of the risk is high. The clean desk and clear screen policy, the secure storage policies, and the data handling rules are designed to protect the highly sensitive personal data that Tusla's functions require it to process. An unauthorised disclosure of this type of personal data has the inherent capacity to seriously infringe the rights and freedoms of data subjects. The sensitivity of the personal data is illustrated in BN-18-6-482, which concerned a [redacted]. The number of data subjects that can be affected by a single failure to apply the *"Records Management Policy"* and the *"Information Classification and Handling Policy"* is illustrated in BN-18-7-124, which concerned the special category data of 150 data subjects.

8.67 I find that the risk of non-implementation of the *"Records Management Policy"* or the *"Information Classification and Handling Policy"* poses a high risk to the rights and freedoms of the data subjects. The moderate likelihood of this risk must be balanced with the high severity of the risk. In particular, the capacity for a single instance of non-implementation to result in the unauthorised disclosure of the highly sensitive personal data of many data subjects to unknown recipients results in this risk being classified as high.

ii. Security Measures Implemented by Tusla

8.68 Tusla implemented a number of measures to promote compliance with its *"Records Management Policy"* and *"Information Classification and Handling Policy"*. The policies were accessible to all staff on the Tusla intranet. The Tusla Newscast, a communications channel made available to all staff, was used by Tusla to communicate key data

protection messages to staff, including on the secure storage of data[12]. These communications also directed staff to *"the Hub"*, where various data protection resources were available. Mandatory GDPR training was provided to all staff in 2018, with refresher training in 2019. The principles and core requirements of the GDPR form part of the induction training for all staff.

8.69 The Clean Desk and Clear Screen Policy and the Information Classification and Handling Policy were updated by Tusla for the introduction of the GDPR in May 2018. Furthermore, in its submissions, dated 13th February 2019, Tusla submitted that a due diligence exercise was being undertaken in respect of its data protection policies. Tusla also outlined that there are a number of triggers in place at Tusla for a review of technical and organisational practices, including governance, change projects, and continuous improvement. However, there was no evidence of any Tusla processes being in place to test whether the existing policies were being adhered to and enforced throughout the organisation.

iii. The Appropriate Level of Security

8.70 Having regard to the high risk to the rights and freedoms of natural persons presented by the non-implementation of the *"Records Management Policy"* or the *"Information Classification and Handling Policy"*, I find that an appropriate level of security must include a process for regularly testing whether the policies are being adhered to and enforced throughout the organisation. The process should ensure formalised managerial oversight over, among other things, Tusla's clean desk and clear screen policy, secure storage policies, and data handling rules. Appropriate tests must be devised to ensure that staff are complying with these policies throughout the organisation.

8.71 Such testing may result in the identification of further appropriate technical and organisational measures. For example, if the testing established a systemic failure to securely store documents when being transferred outside Tusla's premises, it would follow that further measures would be necessary to ensure that the policies are followed. Such measures could include further staff training and enforcement of the policies. Tusla's governance, change projects, and continuous improvement review processes, as set out in its submissions dated 13th February 2019 are not sufficient because, although they establish triggers to review such policies, they do not provide a process for testing the implementation of existing policies.

8.72 I have had regard to the likely cost of implementing such a process. I find that implementing such a process would not impose a disproportionate cost on Tusla with regard to their obligation to implement a level of security appropriate to the risk presented.

[12] Newscast dated 22nd February 2018.

iv. Finding

8.73 I find that Tusla infringed Article 32(1) of the GDPR by failing to implement a process for regularly testing the effectiveness of its *"Records Management"* and *"Information Classification and Handling Policy"*, including whether the policies are being adhered to and enforced throughout the organisation, in a manner that is appropriate to the risk presented by staff failing to comply with these policies.

F. Data Accuracy: Sharing Personal Data and Updating Tusla Records

Relevant Personal Data Breach Notifications: BN 18-11-74, BN-18-9-156, BN-18-8-333, and BN-18-8-519.

8.74 Breach notifications BN 18-11-74 and BN-18-9-156 concerned instances where Tusla disclosed personal data to third parties that was inaccurate in respect of the data subjects. Breach notifications BN-18-8-333 and BN-18-8-519 concerned instances where Tusla issued letters to incorrect addresses because of inaccurate internal records.

8.75 Article 5(1)(d) of the GDPR provides that personal data shall be:

> *"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')"*

8.76 Whether personal data is accurate, within the meaning of Article 5(1)(d), must be assessed in light of the purpose for which the data was collected. In *Nowak v Data Protection Commissioner*, the Court of Justice of the European Union, considering Article 6(1)(d) of the Data Protection Directive, held that:

> *"It is apparent from Article 6(1)(d) of Directive 95/46 that the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected. That purpose consists, as far as the answers submitted by an examination candidate are concerned, in being able to evaluate the level of knowledge and competence of that candidate at the time of the examination. That level is revealed precisely by any errors in those answers. Consequently, such errors do not represent inaccuracy, within the meaning of Directive 95/46, which would give rise to a right of rectification under Article 12(b) of that directive."*[13]

[13] Case C-434-16, Nowak v Data Protection Commissioner, judgment of 20 December 2017 (ECLI:EU:C:2017:994).

i. Accuracy of Personal Data Disclosed to Third Parties

8.77 Breach notification BN 18-11-74 occurred when Tusla's processor, an organisation under [redacted], issued a placement report to [redacted]. The placement report was generated by copying text from an existing report, without removing all of the existing personal data of an unrelated service user. There were no blank templates in use by the processor for placement reports at the time. Issuing the inaccurate placement report to [redacted] infringed Article 5(1)(d) of the GDPR because it inadvertently misrepresented the personal data of one data subject as the personal data of another data subject. Therefore, it constituted a failure to ensure that personal data is accurate. Pursuant to Article 28(1) of the GDPR, Tusla is obliged to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR. Furthermore, as a controller, Tusla is responsible for any processing of personal data carried out on its behalf pursuant to Article 24 of the GDPR. Tusla is accountable not only for the processor's failure to implement appropriate technical and organisational measures, but also for a failure to adhere to the principle of accuracy in this case.

8.78 Breach BN-18-9-156 occurred when Tusla acquired and shared [redacted] of a child. Tusla inadvertently misrepresented that personal data as the personal data of [redacted] when making a placement request for the intended data subject. The report was shared with two different organisations. Acquiring and sharing this report constitutes a failure to ensure that the personal data of the intended data subject was accurate and is an infringement of Article 5(1)(d).

ii. Accuracy of Tusla's Internal Records

8.79 Breach notification BN-18-8-333 occurred when Tusla sent a letter to the old address of the intended recipient because this was the address that was on Tusla's central database. The intended recipient had informed Tusla that their address had changed before the letter was sent. However, Tusla did not update their own records. The letter was opened by the new residents of the address. Tusla's failure to update the intended recipient's address is an infringement of Article 5(1)(d) of the GDPR.

8.80 Breach notification BN-18-8-519 occurred when Tusla sent apology letters to a data subject for previously issuing a letter to their incorrect address. Both of the apology letters were also sent to the incorrect address. Although this did not result in a personal data breach because the letters were issued by registered post and were returned unopened, the accuracy requirement must be assessed in light of the purpose for which the data was collected. In this regard, I consider that the accuracy of addresses is essential not only for preventing personal data breaches like in BN-18-8-333, but also for ensuring that recipients receive intended correspondence. This is one of the purposes for which the data is collected. Therefore, Tusla infringed Article 5(1)(d) in respect of both of its failures to ensure the accuracy of the addresses of the data subjects in breaches BN-18-8-333 and BN-18-8-519.

iii. Findings

8.81 I find that Tusla infringed Article 5(1)(d) of the GDPR on the four occasions outlined in BN 18-11-74, BN-18-9-156, BN-18-8-333, and BN-18-8-519 by failing to ensure that the personal data that it processed was accurate and, where necessary, kept up to date.

G. Duty to Notify Personal Data Breaches

Relevant Personal Data Breach Notifications: BN-18-8-146, BN 18-11-74, BN-18-7-303, BN-18-9-156, BN-18-6-288, BN-18-6-482, BN-18-8-244, BN-18-9-480, BN-18-8-519 and BN-18-6-483.

8.82 Tusla notified the DPC of all of the personal data breaches considered in this Decision pursuant to its obligation under Article 33(1) of the GDPR. However, notifications must occur without undue delay. Most of the personal data breaches were notified within 72 hours. This part considers the personal data beaches that were notified outside the 72 hour period provided for in Article 33(1). Notifying outside the 72 hour period does not *per se* constitute an infringement of Article 33(1) because that Article acknowledges that it will not always be feasible to notify within 72 hours. Therefore, this Decision must consider whether, in each individual case, there was an undue delay in notifying the DPC outside the 72 hour period. The amount of time between Tusla becoming aware and notifying the DPC in those cases ranges from 6 days to 6 weeks. In the breach notification forms, Tusla submitted various reasons for not notifying the DPC within 72 hours. However, it was regularly the case that the reason for the delay was that the Tusla staff member involved in the personal data breach did not notify Tusla's data protection unit immediately.

i. The Obligation to Notify Without Undue Delay

8.83 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."*

8.84 The obligation to notify the DPC applies to all personal data breaches, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Article 4(12) defines personal data breach:

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

8.85 Article 33(1) requires that notifications must occur without undue delay. What constitutes undue delay must be assessed from when Tusla became aware of each personal data breach. The Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679[14] 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."[15]

8.86 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." [16]

8.87 A controller is taken to be aware of a personal data breach from when any member of its staff becomes aware of it. The awareness cannot be inferred from when the data protection unit becomes aware of it. If the person who becomes aware is not responsible for handling personal data breaches, that staff member must ensure that the information is immediately shared with the responsible unit. Indeed, this requirement is implemented into Tusla's Privacy Policy, which requires that all potential data breaches are notified to their Data Protection Unit as soon as they become aware of same. Where a controller becomes aware of an incident that may be a personal data breach, controllers must promptly investigate the incident to determine whether personal data have been breached.

ii. The Breach Notifications

Breach BN-18-8-146

8.88 Breach BN-18-8-146 occurred when a Tusla employee emailed a list of service users to a distribution list of 25 employees of the HSE on 30th July 2018. The intended recipient was another Tusla employee. Tusla became aware of the breach on 30th July 2018 and notified the DPC on 7th August 2018. Tusla stated that there was a delay in notifying the DPC due to an administrative error.

[14] Article 29 Working Party, Guidelines on Personal Data breach notification under Regulation 2016/679, Adopted 6 February 2018.

[15] Ibid at page 10.

[16] Ibid at page 11.

8.89 This breach created a risk to the rights and freedoms of the data subjects. The list in question concerned service users in the [redacted]. This personal data has the potential to be highly sensitive in some instances. The recipients of the unauthorised disclosure are likely to be trusted recipients. However, the large number of recipients increases the risk. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.90 Tusla notified the DPC 8 days after it became aware of this breach. In the circumstances, this 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. An administrative error does not relieve Tusla of the obligation to notify within 72 hours of becoming aware. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach within 72 hours of becoming aware of it.

Breach BN-18-11-74

8.91 Breach BN 18-11-74 occurred on 18th October 2018 when Tusla's processor, an organisation under the name [redacted], issued a placement report to [redacted]. The placement report was generated by copying text from an existing report, without removing all of the existing personal data of an unrelated service user. Tusla became aware of the breach on 18th October 2018 and notified the DPC on 6th November 2018. In the breach notification form the reason for not notifying within 72 hours was explained as *"It was not clear if a breach had occurred until the matter was investigated further."* The placement report did not contain the name of the data subject whose personal data was inaccurately included in the report, but Tusla submitted that that data subject may be identifiable based on the nature of the report.

8.92 This personal data breach created a risk to the rights and freedoms of both the intended subject of the report and the individual whose personal data was copied into the report. The breach notification indicates that special categories of personal data were involved and that vulnerable data subjects were affected. The risk posed by this breach concerns not only the unauthorised disclosure of the personal data of the potentially identifiable data subject, but also the inaccurate transmission of the identified data subject's personal data.

8.93 Article 33(2) requires processors to notify controllers without undue delay after becoming aware of a personal data breach. It appears that this occurred in this instance as Tusla became aware of the breach on the same day that it occurred. The obligation to notify under Article 33(1) rests with the controller. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.94 Tusla notified the DPC 18 days after it became aware of this breach. In the circumstances, this constitutes an undue delay. It was necessary for Tusla to investigate further to determine if a personal data breach had occurred. However, there was an obligation on Tusla to take prompt action to investigate whether personal data had in fact been breached. It should have become clear to Tusla soon after becoming aware of the incident

that a personal data breach had occurred and that there was a risk to the rights and freedoms of the data subjects. The circumstances of this personal data breach, including the involvement of a processor and the original lack of clarity as to whether one of the data subjects was identifiable, does not justify an 18 day delay in notifying the DPC from when Tusla became aware of a potential breach. This was an undue delay. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach without undue delay.

Breach BN-18-303

8.95 Breach BN-18-7-303 occurred on 11th June 2018 when Tusla sent case conference minutes to a [redacted] working in the HSE. The minutes included personal data of 5 children, but the [redacted] should have received the minutes in relation to one child only. Tusla submitted in its breach notification form that the breach was detected on 12th July 2018. That is the same date that the staff member notified the Tusla data protection unit of the breach. Tusla notified the DPC on 13th July 2018.

8.96 This breach created a risk to the rights and freedoms of the data subjects. Although the recipient is a trusted recipient, the personal data disclosed concerns case conference minutes and is likely highly sensitive. Furthermore, the breach concerned the personal data of 4 vulnerable data subjects. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.97 Tusla became aware of the breach on 11th June 2018. As outlined above, a controller is taken to become aware of a personal data breach from when any member of its staff becomes aware of it, even if that member of staff is not responsible for handling personal data breaches. Tusla cannot rely on its own staff member's delay in communicating the breach to the data protection unit as a basis for extending the requirement to notify within 72 hours where feasible.

8.98 Tusla notified the DPC over one month after becoming aware of the breach. In the circumstances, this constitutes an undue delay. A period in excess of a month 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 becoming aware of it. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach without undue delay.

Breach BN-18-9-156

8.99 Breach BN-18-9-156 occurred on 4th June 2018 when Tusla contacted [redacted] seeking the [redacted] of a child. In error, Tusla contacted [redacted] and was furnished with the personal data of another child with the same name. The personal data of that child was subsequently used for a placement request and in referral forms [redacted] The breach was detected by Tusla on 26th

July 2018 and it notified the DPC on 6th September 2018. The data protection unit in Tusla was informed of the breach by the relevant staff member on 5th September 2018.

8.100 This breach created a risk to the rights and freedoms of the data subject. The personal data breach concerns not only Tusla's own accidental access to [redacted], but also its onward disclosure to other organisations. The context of this disclosure heightens the risk to the rights and freedoms of the data subject. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.101 Tusla notified the DPC 6 weeks after becoming aware of the breach. In the circumstances, this constitutes an undue delay. A period of 6 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. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach within 72 hours of becoming aware of it.

Breach BN-18-6-288

8.102 Breach BN-18-6-288 occurred on 27th May 2018 when Tusla sent a letter to an individual against whom [redacted] had been made. The purpose of the letter was to inform that individual that [redacted] However, the letter inadvertently contained the name of another individual, stating that a [redacted] had been made against that individual. The social work team became aware of the breach on 5th June 2018 and notified Tusla's data protection unit on 12th June 2018. Tusla's data protection unit notified the DPC on the same day.

8.103 This breach created a risk to the rights and freedoms of the data subject. The personal data disclosed is highly sensitive and concerns [redacted] Furthermore, the recipient of the personal data is not a trusted recipient and, at the time of the breach notification, the letter had not been retrieved from the recipient. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.104 Tusla notified the DPC 7 days after becoming aware of the breach. In the circumstances this 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, and, as noted above, the delay of the internal notification to Tusla's data protection unit does not justify an extension of the 72 hour period. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach within 72 hours of becoming aware of it.

Breach BN-18-6-482

8.105 Breach BN-18-6-482 occurred on 16th June 2018 when the door to an office in a Tusla [redacted] was left open and a [redacted] there accessed a [redacted] in relation to themselves. [redacted] may have also had the opportunity to view other client files. The breach was detected immediately as the [redacted]

[redacted] was observed accessing the file. Tusla notified the DPC on 25th June 2018. Tusla's data protection unit was notified of the breach on 21st June 2018.

8.106 It is unclear whether the [redacted] accessed personal data relating to anybody else. However, the definition of *"personal data breach"* in Article 4(12) include breaches of security leading to unauthorised access to personal data and is not limited to circumstances where a third party is involved in an unauthorised disclosure of personal data. Furthermore, the personal data breach created a risk to the rights and freedoms of the data subject. The unauthorised viewing of the [redacted] without any supervision or appropriate medical support, created a risk to the rights and freedoms of the data subject. Therefore, Tusla was under an obligation to notify the DPC of this breach without undue delay.

8.107 Tusla notified the DPC 9 days after becoming aware of the breach. In the circumstances this 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, and, as noted above, the delay of the internal notification to Tusla's data protection unit does not justify an extension of the 72 hour period. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach within 72 hours of becoming aware of it.

Breach BN-18-8-244

8.108 Breach BN-18-8-244 occurred on 19th July 2018 when Tusla issued two letters to the wrong address in the same area as the intended recipient. The letters identified a [redacted], referenced the involvement of social workers, and the nature of a concern that Tusla had regarding child protection. Tusla became aware of the breach on 8th August 2018 when a social worker met the [redacted] and asked why they hadn't responded to the letters. The notification to the DPC was prepared on 10th August 2018, but due to an administrative error, was not submitted to the DPC until 14th August 2018.

8.109 This breach created a risk to the rights and freedoms of the data subjects. The personal data disclosed in highly sensitive, and it was disclosed to a recipient who lives in the [redacted] and may be known to them. Furthermore, at the time of the breach notification, the letters had not been retrieved. It also appears that the personal data of at least one child and vulnerable data subject was disclosed. Therefore, there was an obligation on Tusla to notify the DPC of this breach without undue delay.

8.110 Tusla notified the DPC 6 days after becoming aware of the breach. In the circumstances this 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. An administrative error is not a ground for extending the standard 72 hour period. Therefore, Tusla infringed Article 33(1) by failing to notify the DPC of this breach without undue delay.

BN-18-9-480

8.111 Breach BN-18-9-480 occurred on 10th July 2018 when Tusla disclosed the phone number and the location of a data subject when responding to a freedom of information request made by the [redacted] Tusla became aware of the breach on 24th August 2018 when the Tusla Corporate FOI office reviewed records that had been released. Tusla notified the DPC of the breach on 27th September 2018. The reason for the delay, as submitted in the breach notification form, was that Tusla was liaising [redacted] *"to investigate if any harm could present to the data subject"*.

8.112 This breach created a risk to the rights and freedoms of the data subject. The risk is particularly high in circumstances where the [redacted] was disclosed to an individual [redacted] been made in respect of the data subject. Furthermore, this individual was known by Tusla to have made attempts to contact the data subject in the past.

8.113 Tusla notified the DPC 4 weeks and 6 days after becoming aware of the breach. In the circumstance, this constitutes an undue delay. Such a delay is not justifiable by reference to Tusla's efforts to investigate whether harm could present to the data subject. While it is not always immediately apparent whether a personal data breach is "*unlikely to result in a risk to the rights and freedoms of natural persons"*, in such circumstances, the emphasis should be on prompt action to investigate. Tusla's delay of over 4 weeks is entirely unjustifiable in the circumstances.

BN-18-8-519

8.114 Breach notification BN-18-8-519 relates to an incident that occurred on an unknown date in May/June 2018 and on 11th June 2018 when Tusla issued two apology letters to the wrong address of a service user. The apology related to a similar mistake that occurred prior to the GDPR coming into force. The letters were issued by registered post and were returned unopened.

8.115 The obligation to notify under Article 33(1) applies to personal data breaches only. Article 4(12) of the GDPR defines *"personal data breach"* as follows:

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

8.116 The sending of the apology letters did not lead to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Therefore, no personal data breach occurred in this instance and there was no obligation on Tusla to notify the DPC of the incident. As a result, Tusla did not infringe Article 33(1) by failing to notify the DPC without undue delay. This is without prejudice to Tusla's obligation regarding the accuracy of personal data under Article 5(1)(d) of the GDPR.

BN-18-6-483

8.117 Breach notification BN-18-6-483 relates to an incident that occurred on 21st June 2018 when Tusla sent an email to an incorrect colleague within Tusla. The colleague immediately deleted the email in an unread and unopened state. In the breach notification form, Tusla submitted:

> *"Unfortunately the unit where the breach occurred, did not notify the DPO team within the required 72 hour period."*

8.118 In circumstances where Tusla was able to confirm that the email was deleted before being read or opened, I am satisfied that there was no destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Therefore, a personal data breach did not occur and Tusla was not obliged to notify the DPC of this incident. As a result, Tusla did not infringe Article 33(1) by failing to notify the DPC without undue delay.

iii. Findings

8.119 I find that Tusla infringed Article 33(1) of the GDPR on 8 occasions by failing to notify the personal data breaches detailed in breach notifications BN-18-8-146, BN 18-11-74, BN-18-7-303, BN-18-9-156, BN-18-6-288, BN-18-6-482, BN-18-8-244 and BN-18-9-480 without undue delay.

8.120 I find that Tusla did not infringe Article 33(1) in respect of notifying the DPC of the incidents detailed in breach notifications BN-18-8-519 and BN-18-6-483.

H. Remaining Breach Notifications

8.121 The Inquiry Commencement Letter outlined that it was commenced having regard to the notified personal data breaches and to establish a full set of facts so that it may assess whether or not Tusla has discharged its obligations as data controller and/or data processor in connection with the subject matter of the breaches. As outlined above, this Decision considers all of the information obtained in the Inquiry, including the information obtained in relation to the personal data breaches, in determining whether infringements have occurred or are occurring. It does not necessarily follow from a notification of a personal data breach that the breach was caused by an infringement of the GDPR or the 2018 Act. However, for the sake of clarity, having considered all of the information obtained in course of the Inquiry, this Decision finds that the following notified personal data breaches did not present any probative information suggesting that an infringement to which the inquiry relates has occurred or is occurring. This is in addition to the breach notifications that were excluded from consideration for the reasons set out in Part 3.

Relevant Personal Data Breach Notifications: BN-18-8-416, BN-18-11-73, BN-18-6-18, BN-18-6-40, BN-18-6-123, BN-18-6-239, BN-18-6-484, and BN-18-8-554.

8.122 Notifications BN-18-6-416 and BN-18-11-73 concerned personal data being misplaced by service users in circumstances that were outside the control of Tusla. Notifications BN-18-6-239 and BN-18-6-484 concerned the loss and theft of Tusla mobile phones where the phones were password protected, encrypted and had remote wipe functionality and no personal data breach occurred in either case. BN-18-6-123 concerned an unsuccessful attempt at phising where no personal data was compromised. Notifications BN-18-8-554 and BN-18-6-40 concern lawful disclosures of personal data. BN-18-9-345 concerns a personal data breach regarding a controller other than Tusla. Breach BN-18-6-18 was an incident where boxes were physically damages during transit by a courier company because the boxes were stored at the bottom of a crate. There was no data protection issue arising in this instance.

9. Corrective Powers

9.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that Tusla has infringed Article 5(1)(d), 32(1), 32(4), and 33(1) of the GDPR. Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with Section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. 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, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2):

a) Article 58(2)(b) – I have decided to issue a reprimand to Tusla in respect of its infringements of Articles 5(1)(d), 32(1), 32(4), and 33(1);
b) Article 58(2)(d) – I have decided to order Tusla to bring its processing into compliance with Article 32(1) of the GDPR;
c) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of Tusla's infringements of Article 32(1) regarding processing operations concerning the internal and external transmission of personal data and its failure to implement a process for regularly testing the effectiveness of its existing policies, and its infringements of Article 33(1) of the GDPR; and
d) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of Tusla's infringement of Article 32(1) regarding its printing and scanning processing operation.

A. Reprimand

9.2 I issue Tusla with a reprimand under Article 58(2)(b) of the GDPR regarding its infringements of Articles 5(1)(d), 32(1), 32(4), and 33(1) of the GDPR. In imposing a corrective power, and in accordance with Recital 129, I must ensure that it is *"…necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…".* In this respect, in deciding to impose a reprimand in addition to an order to Tusla to bring its processing into compliance and an administrative fine, I have had particular regard to the nature of Tusla's failure to provide an appropriate level of security, to take steps to ensure that persons acting under Tusla's authority do not process personal data except on their instructions, to notify the personal data breaches to the DPC without undue delay, and to ensure the accuracy of personal data. In light of the potential for highly sensitive personal data to be affected, and the need to re-establish compliance with the GDPR and dissuade non-compliance, I consider that the imposition of reprimand is both necessary and proportionate taking into account the circumstances of this individual case.

B. Order to Bring Processing into Compliance

9.3 In addition to the reprimand in respect of the infringements of Articles 32(1), in accordance with Article 58(2)(d) of the GDPR, I order Tusla to bring the processing operations, identified in this Decision, into compliance with Article 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks. In this regard, I acknowledge Tusla's on-going remedial actions and strategic transformation, as outlined in submissions throughout the Inquiry. However, this order is necessary and proportionate in light of the importance of ensuring that full effect is given to Tusla's obligation to implement appropriate technical and organisational measures, having particular regard to the high quantity, high sensitive, personal data of vulnerable data subjects processed by Tusla. Tusla should perform the necessary risk assessments to inform the measures that it must implement, and must continually evaluate the dynamic risks in assessing which technical and organisational measures it is obliged to implement. However, as outlined above regarding the assessment of risk in this Decision, those measures must include:

(i) A display message at every user logon to the NCCIS;
(ii) Specific instruction to all staff at induction and regular training to existing staff regarding the issue of inappropriate access to personal data encountered during the course of their employment;
(iii) Regular national and local auditing of the access logs to the NCCIS,
(iv) A technical measure that specifically addresses the risk posed by HSE email addresses being included in the global address lists. The *"Tusla only"* email infrastructure, which was not in place at the time of the infringements, is sufficient for these purposes;

(v) Co-ordinated national templates for commonly issued letters and forms in web-based forms that automatically revert to empty when correspondence is issued;

(vi) A policy that mandates sensitive personal data transmitted by internal and external email to be password protected, subject to any exceptions to this policy that may be necessary in light of Tusla's need to exchange information urgently between staff, including in relation to urgent child protection incidents. The precise exceptions to the policy must be informed by Tusla's risk assessment;

(vii) A policy that mandates a second review of letters containing sensitive personal data where it is not feasible to send those letters by via email in a password protected manner;

(viii) Fully implemented organisation-wide secure print facilities and secure scan facilities; and

(ix) A process for regularly testing the effectiveness of its *"Records Management"* and *"Information Classification and Handling Policy"*.

9.4 In determining the time scale for Tusla to comply with this order by implementing appropriate technical and organisational measures, I have had regard to Tusla's submissions on the Draft Decision. Those submissions set out the complex operating environment that relates to Tusla. The submissions also detailed some of the challenges faced by Tusla surrounding the current Covid-19 crisis, including the delivery of critical services to children and families, the need to redeploy staff who are integral to the implementation of Tusla's action plan, and the impact on cross-organisational actions because of the majority of staff working remotely. Tusla's submissions set out the following target completion dates in respect of the above identified measures:

Measure	Target Completion
(i) A display message at every user logon to the NCCIS	30th September 2020
(ii) Specific instruction to all staff at induction and regular training to existing staff regarding the issue of inappropriate access to personal data encountered during the course of their employment;	Q3 2020 and ongoing
(iii) Regular national and local auditing of the access logs to the NCCIS,	31st December 2020
(iv) A technical measure that specifically addresses the risk posed by HSE email addresses being included in the global address lists. The *"Tusla only"* email infrastructure, which was not in place at the time of the infringements, is sufficient for these purposes;	31st December 2021
(v) Co-ordinated national templates for commonly issued letters and forms in web-based forms that automatically revert to empty when correspondence is issued;	31st December 2020
(vi) A policy that mandates sensitive personal data transmitted by internal and	31st October 2020

external email to be password protected, subject to any exceptions to this policy that may be necessary in light of Tusla's need to exchange information urgently between staff, including in relation to urgent child protection incidents. The precise exceptions to the policy must be informed by Tusla's risk assessment;	
(vii) A policy that mandates a second review of letters containing sensitive personal data where it is not feasible to send those letters by via email in a password protected manner;	31st October 2020
(viii) Fully implemented organisation-wide secure print facilities and secure scan facilities;	30th September 2021
(ix) A process for regularly testing the effectiveness of its "Records Management" and "Information Classification and Handling Policy".	Ongoing

9.5 I am satisfied that the timelines proposed by Tusla are reasonable in the particular circumstances. Therefore, I order Tusla to bring its relevant processing operations into compliance with Article 32(1) of the GDPR by 31st December 2021. I direct that Tusla must submit reports to the DPC outlining the steps it has taken in respect of each of the measures on or before their respective deadlines, being 30th September 2020, 31st October 2020, 31st December 2020, 30th September 2021, and 31st December 2021. [redacted]

C. Administrative Fines

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

i. Decision to Impose Administrative Fines

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

> *"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 As outlined above, this Decision finds 5 infringements of Article 32(1), in respect of 5 of Tusla's processing operations. Those processing operations are extensive in some instances, but can be generally summarised as: Tusla's transmission of personal data on the NCCIS; Tusla's transmission of personal data internally by email; Tusla's transmission of personal data externally using post and email, including the use of template letters and forms; Tusla's printing and scanning processing operations; and the processing operations subject to Tusla's *"Records Management Policy"* and *"Information Classification and Handling Policy"*.

9.9 In determining whether to impose administrative fines, each infringement must be considered separately. This Decision will apply the criteria set out in Article 83(2) of the GDPR to each infringement of Article 32(1) and Article 33(1). However, where possible, the consideration of each criterion will be grouped for the different infringements. The decision as to whether to impose an administrative fine in respect of an infringement (and if so, the

amount of the fine) must be a cumulative decision which is taken having regard to each of the range of factors as set out in Article 83(2)(a) to (k). While the decision as to whether to impose an administrative fine must be distinct in respect of each infringement, where the infringements relate to linked processing operations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement in accordance with Article 83(3) GDPR. I will now proceed to consider each of the criteria set out in Article 83(2)(a) to (k) in turn in respect of Tusla's infringements of Articles 32(1) and 33(1) of the GDPR respectively.

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

9.10 The nature of the infringements 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 technical and organisational measures must also be assessed in light of the risks posed to the rights and freedoms of data subjects regarding each relevant processing operation. Tusla processes highly sensitive personal data on the NCCIS, by internal email, by external transmission, and through printing and scanning. The breach notifications considered in respect each infringement illustrate the sensitivity of the data processed. The nature of the processing must also be assessed in light of its purpose, which is reflected in Tusla's functions of providing child welfare and protection services. Such purposes reflect the serious nature of the infringements because unauthorised disclosures of personal data processed in this context has significant capacity to cause material and non-material damage to data subjects. A large number of data subjects could potentially be affected by the lack of appropriate security in respect of each one of the processing operations because Tusla has State-wide responsibility for improving wellbeing and outcomes for children. 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).

9.11 The nature of the infringements of Article 33(1) must also be assessed in light of the fact that such infringements are usually capped at the lower threshold under Article 83(4). However, the nature of these infringements 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 , for example ordering a controller to communicate a personal data breach to affected data subjects under Article 58(2)(e) of the GDPR. Each of the personal data breaches concern vulnerable data subjects.

Furthermore, they all involved sensitive or highly sensitive personal data. An undue delay in notifying such personal data breaches could pose a significant risk to the rights and freedoms of data subjects. In those circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the infringements of Article 33(1) is serious in nature.

9.12 The gravity of the infringement of Article 32(1) in respect of Tusla's processing on the NCCIS is serious in circumstances where it is directly attributable to personal data breach BN-18-11-166. The lack of appropriate technical measures to prevent staff from accessing personal data [redacted] is of serious gravity, which likely resulted in a high level of damage to the data subjects.

9.13 The gravity of the infringement of Article 32(1) in respect of Tusla's transmission of personal data internally by email is moderate. This infringement directly resulted in 10 personal data breaches, with a large number of affected data subjects. The gravity of the infringement is mitigated in light of the potential for trusted recipients being involved in some of the personal data breaches stemming from this infringement. This reduces the likely level of damage suffered by data subjects as a result of the infringement. Nonetheless, the gravity is moderate because of the potential for serious personal data breaches, such as the disclosure of a protected disclosure concerning Tusla to the national public health service (BN-18-6-227).

9.14 The gravity of the infringement of Article 32(1) in respect of Tusla's external transmission of personal data is serious. This infringement contributed to 28 personal data breaches. The likely level of damage suffered by the data subjects is aggravated because of the sensitivity involved in many of the breaches, the lack of control that Tusla operates over the recipients of the personal data, and the fact that, in at least on instance, the identity of the recipient was unknown.

9.15 The gravity of the infringement of Article 32(1) in respect of Tusla's printing and scanning processing operations is moderate. This infringement resulted in three personal data breaches. The likely level of damage suffered by the data subject in one of the breaches is low in circumstances where the failure of the secure print facility to engage resulted in another Tusla staff member having unauthorised access to personal data in good faith. However, this must be balanced with the higher level of potential damage in the scanning disclosure, which concerned special category personal data and an external recipient, and the higher level of potential damage in BN-18-8-184.

9.16 The gravity of the infringement of Article 32(1) in respect of Tusla's failure to implement a process for regularly testing the effectiveness of its *"Records Management"* and *"Information Classification and Handling Policy"* is serious. This failure contributed to 6 personal data breaches, including one that involved special category personal data and 150 data subjects. Although the personal data was recovered the next day, the loss of control suffered by the data subjects is serious.

9.17 The gravity of the infringements of Article 33(1) are all serious. The shortest delay occurred where Tusla notified the DPC 6 days after becoming aware of a personal data breach. Even this shortest infringement is double the 72 hour period provided for in Section 33(1). The longest delay occurred where Tusla notified the DPC 6 weeks after becoming aware of a personal data breach. The remainder of the infringements varied between 6 days and 6 weeks. The delays had the capacity to prevent full mitigation of the personal data breaches and, therefore, the gravity of the infringements are serious.

9.18 The duration of the infringements of Article 32(1) commenced at the coming into force of the GDPR on 25th May 2018 because the appropriate technical and organisational measures were not implemented at that time. In circumstances where Tusla is currently undertaking significant remedial actions and a strategic transformation, it is not possible to pinpoint exactly when the failure to implement appropriate technical and organisational measures concluded in respect of each infringement. However, having regard to the target completion date in Tusla's action plan[17], it is clear that the infringements were ongoing at the commencement of the Inquiry on 6th December 2018 because the measures that ought to have been implemented, as outlined in this Decision, were not in place at that date. Therefore, the duration of all of the infringements is, at a minimum, 27 weeks in length. In the context of infringements of Article 32(1) of the GDPR, this duration is moderate.

9.19 Regarding the duration of the infringements of Article 33(1), as outlined above, there are no circumstances concerning any of the breaches that justice a failure to notify the DPC within 72 hours of becoming aware of each breach. Therefore, the duration of each infringement equates to the amount of time that it took Tusla to notify from becoming aware of each breach deducted by 72 hours. Therefore, the duration of the infringements concerning BN-18-8-244, BN-18-6-288, BN-18-8-146, and BN-18-6-482 were between 4 and 6 days, which I consider moderate in the circumstances. The duration of the infringements in BN-18-11-74, BN-18-303, BN-18-9-156 and BN-18-9-480 were between 15 days and 39 days, which I consider serious in the circumstances.

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

9.20 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."*

9.21 Regarding Tusla's infringements of Article 32(1) in respect of its processing operations concerning the transmission of personal data and its printing and scanning processing operation, I am satisfied that each infringement was negligent in character, but that they were not intentional. The failure to implement the technical and organisational measures

[17] Tusla's Response to the DPC's Draft Inquiry Report (IN-18-11-04), dated 28th February 2020.

identified in this Decision breached the duty of care owed by Tusla. However, I am satisfied that the failure to implement the measures was not done with the knowledge of an infringement of Article 32(1) and the infringement was not wilful on the part of Tusla.

9.22 Regarding Tusla's failure to implement a process for regularly testing the effectiveness of its *"Records Management Policy"* or the *"Information Classification and Handling Policy"*, the Administrative Fines Guidelines indicate that a failure to read and abide by existing policies is indicative of unintentional, or negligent, conduct[18]. While a failure to read and abide by the *"Records Management Policy"* and the *"Information Classification and Handling Policy"* was a cause of BN-18-6-482, BN-18-7-471, and BN-18-7-124, the infringement of Article 32(1) in this instance relates to a failure to regularly test the effectiveness of the policies. A systemic organisational failure to apply existing policies may be indicative of contempt for those provisions. However, in this instance, I am satisfied that this infringement was negligent rather than intentional. I have had regard to how the policies were updated for the introduction of the GDPR, shortly before the relevant personal data breaches, and the significance of the measures contained in the policies for protecting personal data if implemented. This illustrates a wilfulness from Tusla to comply with its obligations and that the infringement in this instance was not done with knowledge or wilfulness of the infringement.

9.23 Regarding the infringements of Article 33(1), it is clear in each case that the undue delay was unintentional but negligent. The most common cause of the infringements was that the Tusla staff member involved in a personal data breach delayed notifying Tusla's data protection unit. Tusla's data protection unit acted promptly once they became aware of each breach. I am satisfied that the delay in each case was not attributable to knowledge or a wilfulness to disregard the obligations under Article 33(1).

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

9.24 Regarding the infringement of Article 32(1) in respect of Tusla's transmission of personal data on the NCCIS, this resulted in personal data breach BN-18-11-166. This incident has the potential to cause significant damage to the data subjects in circumstances where it involved a Tusla employee accessing personal data [redacted]. This could undermine the data subjects' trust in Tusla, which would be highly damaging to the data subjects in circumstances where it appears that they are also service users of Tusla. Tusla became aware of the breach when the data subject complained. It is acknowledged that [redacted] However, there is no evidence of any action taken by Tusla to mitigate the damage suffered by the data subjects. There is no evidence of any action to reassure the data subjects' trust and confidence in Tusla as service users. The breach notification form stated that it was not yet known if the employee made printouts from the NCCIS. There is

[18] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 12.

no evidence of any steps taken by Tusla to confirm this or to retrieve such printouts if they were made. Therefore, I cannot find that Tusla took action to mitigate the damage suffered by data subjects in respect of this infringement.

9.25 Regarding the infringement of Article 32(1) in respect of Tusla's transmission of personal data internally by email, this infringement resulted in 10 personal data breaches. As illustrated above, these personal data breaches illustrate the potential for damage to data subjects. I am satisfied that Tusla took significant action to mitigate the damage suffered. Tusla was able to confirm that the relevant emails had been deleted in BN-18-6-534, BN-18-6-53, BN-18-6-571, BN-18-8-316, BN-18-7-266 and BN-18-8-236. In BN-18-8-146, the email was recalled and the recipients were asked to delete it. In BN-18-8-339, the recipient returned the referral letter. The email was recalled in BN-18-7-603 and Tusla was able to confirm that [redacted], so had not yet opened the email. Tusla's prompt action in recalling the disclosed personal data in each of these infringements is mitigating. However, in respect of BN-18-6-227, which concerns a protected disclosure, the recipient was asked to delete the email and confirm that it has been deleted, but there is no evidence that this was complied with.

9.26 Regarding the infringement of Article 32(1) in respect of Tusla's external transmission of personal data, this infringement resulted in a significant number of personal data breaches, which illustrate the potential for damage to data subjects. The action taken by Tusla to mitigate this damage varies across the various personal data breaches. For example, in BN-18-6-549 Tusla confirmed that the letter sent to the wrong address was retrieved and provided to the correct recipient. In BN-19-11-74, the recipient of the emailed report was asked to delete it. Tusla's attempts to retrieve the disclosed personal data each relevant personal data breach is mitigating. Furthermore, where appropriate, Tusla notified the data subjects of the personal data breaches pursuant to Article 34 of the GDPR, for example BN-18-8-476. Such a step can be significant in mitigating the damage suffered by data subjects in certain circumstances. However, for an action carried out by a controller to be considered a mitigating factor, it must be a voluntary remedial action, whereby the controller takes *"responsibility to correct or limit the impact of their actions"*[19]. An action, taken by a controller where it is mandated to do so on foot of a statutory obligation is not a mitigating factor for these purposes.

9.27 Regarding the infringement of Article 32(1) in respect of Tusla's printing and scanning processing operation, this infringement resulted in 3 personal data breaches. Regarding BN-18-8-536, Tusla contacted the incorrect recipient of the scanned document and asked them to delete it. There was no response to this request. Regarding BN-18-6-584, the staff member who accessed the personal data at the printer notified the team that was responsible, allowing the documents to be recovered. Regarding BN-18-8-184, the standard report form was promptly returned to the correct area after being discovered.

[19] Administrative Fines Guidelines, page 13.

9.28 Regarding the infringement of Article 32(1) in respect of Tusla's failure to implement a process for regularly testing the effectiveness of its *"Records Management Policy"* or the *"Information Classification and Handling Policy"*, this infringement contributed to 6 personal data breaches. Regarding BN-18-6-482, Tusla took action to *"Ensure that there are no adverse psychological/emotional/physical/mental effects on the data subject as a result of the report about themselves that they viewed".* Regarding BN-18-7-471, Tusla initiated an investigation into the incident where a [redacted] missing and notified the data subjects pursuant to their obligation under Article 34, which, as detailed above cannot be considered mitigating. There is no evidence of any other action taken by Tusla to mitigate the damage. Regarding BN-18-7-124, [redacted] with 150 data subjects' personal data was retrieved by Tusla within 24 hours. Tusla also undertook a resource-intense task of identifying all of the data subjects and establishing the chain of custody in seeking to determine the extent of the resulting unauthorised disclosure. Tusla liaised with the Gardaí and the relevant taxi company in seeking to locate the form in BN-18-10-115, however such efforts were unsuccessful. Regarding BN-18-8-29, a new online system was implemented for submitting time sheets. Regarding BN-18-9-43, Tusla requested the recipient of the email to destroy it, but Tusla has not confirmed that this request was complied with.

9.29 Regarding the infringements of Article 33(1), despite the delay in notifying the DPC of the personal data breaches, Tusla took action to mitigate the damage suffered by the data subjects. This mitigating action relates to the underlying personal data breaches; it does not strictly relate to the infringement of Article 33(1), which concerns delay in notifying the DPC. Nonetheless, Article 83(2)(c) has a broad scope and includes *"any action"* taken to mitigate *"the damage suffered"*. Therefore, where considering an infringement of Article 33(1), I consider that action to mitigate damage caused by the underlying personal data breach, and not only the delay in notifying the DPC, must be considered mitigating in favour of the controller. Regarding BN-18-9-156, Tusla wrote to the agencies that received inaccurate personal data in order to receive confirmation that their personal data processing had ceased. Tusla recovered the meetings of the minutes that were sent to [redacted] in BN-18-7-303. The recipient of the report in BN 18-11-74 was asked to destroy the report. In BN-18-8-146, the email was recalled and the recipients were asked to delete it. Tusla issued correspondence to the solicitor of the incorrect recipient in BN-18-6-288 seeking to retrieve the letter. As outlined above, Tusla took action regarding the well-being of the data subject in BN-18-6-482. In BN-18-8-244, Tusla issued a letter to the incorrect recipient seeking return of the correspondence. In BN-18-9-480, Tusla took steps to safeguard the data subject from potential adverse consequences arising from the breach. However, the delay in taking the actions outlined above reduced the capacity of Tusla's action to mitigate the damage suffered by the data subjects.

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

9.30 Regarding the infringements of Article 32(1), as outlined above Tusla did not implement appropriate technical and organisational measures pursuant to Article 32(1). I consider that Tusla holds a high degree of responsibility for these failures and that the absence of such

measures must be deterred. However, in circumstances where this factor forms the basis for the finding of infringements of Article 32(1) against Tusla, this factor cannot be considered aggravating in respect of those infringements.

9.31 Regarding the infringements 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 these cases, I find that the existence of this organisational measure is mitigating in the circumstances.

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

9.32 Findings of infringements by Tusla of the GDPR have been made in two separate Decisions of DPC (Decision IN-19-10-1, dated 7th April 2020 and Decision IN-19-12-8, dated 21st May 2020). Regarding the infringements of Article 32(1) in those Decisions, the finding of infringements related to the period beginning on 25th May 2018 and concluding on the dates of the personal data breaches, 14th March 2019 and 15th May 2019 respectively. Therefore, as those infringements coincide with and postdate the finding of the infringements of Article 32(1) in this Decision (25th May 2018 - 6th December 2018), I do not consider those infringements *"previous infringements"* and, therefore, they are not considered aggravating for the purposes of this Decision.

9.33 Regarding the infringements of Article 33(1), Decision IN-19-10-1 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. Decision IN-19-12-8 found that Tusla had infringed Article 33(1) of the GDPR by notifying the DPC of a personal data breach 29 weeks after becoming aware of it. That 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. The infringements found in this Decision occurred prior to the infringements of Article 33(1) found in Decisions IN-19-10-1 and IN-19-12-8. Therefore, those infringements are not *"previous infringements"* and cannot be considered aggravating for the purposes of this Decision.

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

9.34 Tusla cooperated fully with the DPC to remedy the infringements of Article 32(1) and to mitigate their adverse effects. Tusla's submissions, dated 28th February 2020, set out a comprehensive plan developed by Tusla's senior leadership team, which sets out technical and organisational measures that it is implementing, to provide a level of security that is appropriate to its processing operations, including, but not limited to the issues identified in this Decision. An updated plan was submitted in Tusla's submissions on the Draft Decision. In addition to the issues identified, on a provisional basis, in the Draft Decision,

Tusla made submissions on the measures that it is implementing in relation to general data protection training on an organisation-wide basis, change management, and staff joiner/leaver processes, amongst other measures. Tusla also made submissions concerning its *"Transformation Programme"* during its presentation to the Inquiry Team on 8th May 2019. This programme includes initiatives for ensuring compliance with the GDPR.

9.35 Tusla also cooperated to remedy the infringements of Article 33(1) and to mitigate their adverse effects. In its management response, dated 13th February 2019, it outlined how it has established a customised risk assessment for the assessment of individual breaches. It also outlined how a breach assessment team now completes a rigorous assessment of all reports made to it through its central reporting channels. Tusla also outlined how its data protection unit has prioritised employee awareness and training on detecting and preventing breaches.

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

9.36 The categories of personal data affected by all of the infringements in this Decision are highly sensitive. This reflects the nature of Tusla's functions, which include, amongst others, the provision of child welfare and protection services; domestic, sexual and gender-based violence services; and Services related to the psychological welfare of children. The processing of sensitive and special category data is intrinsic to these functions. Unauthorised disclosures of the categories of personal data processed by Tusla is likely to cause immediate damage and distress to data subjects. The notified personal data breaches illustrate that all of the processing operations considered in respect of the Article 32(1) infringements concern highly sensitive personal data. This aggravates the infringements of Article 32(1) 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 infringements of Article 33(1) also concern sensitive personal data. This aggravates those infringements because the higher risk to the rights and freedoms of data subjects makes prompt notification to the DPC even more imperative.

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

9.37 The infringements became known to the DPC because Tusla notified the DPC of all of the personal data breaches. The majority of these notifications were made without undue delay and in compliance with its obligations under Article 33(1). The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> *"The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this*

obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor."[20]

9.38 Tusla's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the Article 32(1) infringements. Conversely, the undue delay when notifying the DPC on 8 occasions is not aggravating in circumstances where those infringements are subject to consideration regarding the exercise of 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;

9.39 Corrective powers have not previously been ordered against Tusla with regard to the subject-matter of this Decision. Although corrective powers were exercised in Decisions IN-19-10-1 and IN-19-12-8, ordering Tusla to bring certain processing operations into compliance with Article 32(1), those orders concerned different processing operations and, therefore, do 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;

9.40 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.

9.41 Decisions IN-19-10-1 and IN-19-12-8 each imposed separate administrative fines on Tusla in respect of distinct and non-linked processing operations. While the infringements found in those Decisions are distinct to the findings of infringements found in this Decision, in the particular circumstances of this Decision, I consider the previous fines mitigating. The Administrative Fines Guidelines provide:

"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)."[21]

9.42 In the particular circumstances, regard must be had to the previous fines in order to ensure that the any corrective powers exercised in this Decision are effective, proportional and dissuasive. Since Inquiries IN-18-11-04, IN-19-10-1 and IN-19-12-8 commenced, Tusla has

[20] Administrative Fines Guidelines, page 15.
[21] Administrative Fines Guidelines, page 6.

submitted significant evidence of actions taken to bring its processing operations into compliance with the GDPR. While this factor is considered mitigating in respect of Article 83(2)(f) above, the previously imposed administrative fines are also separately mitigating in the circumstances. The financial burden imposed by those administrative fines are relevant to assessing the utility of subsequent administrative fines in re-establishing compliance. The infringements found in this Decision pre-date or coincide with the infringements found in those Decisions. Therefore, the fines already imposed may be of utility in re-establishing compliance, even in respect of the separate and distinct infringements. I consider that this matter, along with 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.

Conclusion with regard to the Decision as to whether to impose administrative fines

9.43 In its submissions on the Draft Decision, Tusla submitted that this Decision should not impose administrative fines in circumstances where Decisions IN-19-10-1 and IN-19-12-8 have already imposed separate administrative fines. In this regard, Tusla submitted that the objective of discouraging non-compliance has already been discharged by the DPC. Tusla further submitted that it has demonstrated that it is actively making significant efforts to improve its compliance with data protection legislation and that the fines proposed in the Draft Decision would *"not achieve any real benefit or change in that regard, as the required change is already underway irrespective of any additional fines"*[22].

9.44 The findings of infringements in this Decision are distinct, and relate to separate processing operations, to those under consideration in Decisions IN-19-10-1 and IN-19-12-8. However, as considered in relation to the application of Article 83(2)(f) above, I accept that Tusla has fully cooperated and has taken significant steps to remedy the infringements identified in this Decision. In addition to the matters considered under Article 83(2)(f), I further accept Tusla's submission that its engagement with the DPC demonstrates that it is undertaking significant efforts to comply with data protection legislation. Furthermore, as considered in relation to the application of Article 83(2)(k) above, I consider that the financial burden imposed by those administrative fines are relevant to assessing the utility of subsequent administrative fines in re-establishing compliance, particularly where the wrongdoing in question coincides with, and postdates, the period under consideration in this Decision. As outlined above, all of these matters are mitigating, both in respect of the Decision as to whether administrative fines are to be imposed in the circumstances, and, if so, as to the amount of the administrative fines where applicable.

9.45 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context

[22] Tusla's submission on the DPC's Draft Decision, at page 4.

of the objective pursued by the corrective measures[23]. I find that administrative fines are necessary in the particular circumstances of this case in order to effectively achieve the objective of re-establishing compliance with the GDPR. While I accept that Tusla is currently undertaking significant efforts to bring itself into compliance with the issues raised in this Decision and previous decisions, and I further accept Tusla's submission that it is doing so *"irrespective of any additional fines"*[24], the objective of re-establishing compliance must incorporate the need to dissuade future non-compliance.

9.46 Re-establishing compliance and dissuading non-compliance are objectives that must be assessed in the context of the infringements found in this Decision. Article 32(1) of the GDPR places a continuous obligation on controllers and processors to regularly test, assess, and evaluate the effectiveness of the technical and organisational measures that it has implemented. The appropriate level of security must be continually re-assessed in light of the dynamic risk presented by the Tusla's processing and the state of the art. Where appropriate, controllers and processors may be obliged to implement further measures following that testing. Furthermore, Article 33(1) also imposes a continuous obligation to notify the DPC of any occurring personal data breaches without undue delay, unless unlikely to result in a risk to the rights and freedoms of natural persons. Therefore, Tusla's extensive action plan submitted to the DPC cannot ensure future compliance as the state of the art and the nature of Tusla's processing operations and the risk changes, just as compliance with the order in Part 9(B) of this Decision cannot ensure future compliance. Therefore, I do not accept Tusla's submission that a fine would *"not achieve any real benefit or change in that regard, as the required change is already underway irrespective of any additional fines"*[25]. I consider that fines in this case are necessary when considered in light of the continuous nature of compliance with Articles 32(1) and 33(1). In this regard, the fines are necessary to dissuade future non-compliance, which could take the form of an omission to test and evaluate the measures implemented, an omission to implement appropriate measures in light of the on-going testing, or an omission to notify the DPC of personal data breaches without undue delay, amongst others.

9.47 In finding that administrative fines are necessary to re-establish compliance, I have had regard to the range of factors as set out in Article 83(2)(a) to (k) cumulatively and the need to deter non-compliance in a proportionate manner. I have also had regard to all of the corrective powers available in Article 58(2). I consider that the reprimand in part 9(A) of this Decision are of utility in dissuading future non-compliance. However, I consider that, in addition to the reprimand and the order in part 9(B), administrative fines are necessary and proportionate in order to dissuade future non-compliance. In coming to this conclusion, I have had particular regard to the highly sensitive personal data processed by Tusla and the potential for significant damage to vulnerable data subjects (as assessed under Article 83(2)(a) & (g)). In balancing these factors against the mitigating factors, I have

[23] See 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.

[24] Tusla's submission on the DPC's Draft Decision, at page 4.

[25] Tusla's submission on the DPC's Draft Decision, at page 4.

had particular regard to the action taken by Tusla to mitigate the damage suffered by the data subjects, Tulsa's high degree of cooperation with the DPC to remedy the infringements, and the utility of previously issued fines in re-establishing compliance and dissuading future non-compliance (as assessed under Article 83(2)(c), (f) and (k) respectively). In light of the nature of the infringements and the scale and complexity of Tusla's processing operations, I find that administrative fines are necessary to effectively dissuade non-compliance. Furthermore, in light of scale of non-compliance across Tusla's processing operations found in this Decision, and the seriousness of the resulting personal data breaches, I am satisfied that the imposition of administrative fines is proportionate to that objective.

9.48 Having had due regard to the factors set out above, I have decided that each of the infringements of Article 32(1) and each of the infringements of Article 33(1) warrant the imposition of administrative fines in the circumstances of this case. I must therefore, next proceed to determine whether any of the infringements concern the same or linked processing operations. If so, the amount of the administrative fine for those infringements must not exceed the amount specified for the gravest infringement in accordance with Article 83(3) of the GDPR. Finally, I must proceed to calculate administrative fines that are effective, proportionate and dissuasive, taking into account factors a – k.

ii. Linked Processing Operations

9.49 Article 83(3) of the GDPR provides:

> *"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.*

9.50 The findings of infringements of Article 32(1) in this Decision regarding Tusla's transmission of personal data concern distinct processing operations. Each operation utilises different tools in transmitting personal data and there are different classes of recipients applicable across the operations. However, it is necessary to consider whether those processing operations are *"linked"* for the purposes of Article 83(3). I consider that Tusla's transmission of personal data on the NCCIS, internally by email, and externally using post and email are linked processing operations. Those processing operations all share the same purpose: they are undertaken by Tusla to transmit personal data between stakeholders in order to facilitate it in carrying out its statutory functions. The nature of the processing operations are also linked. The inherent features of all of the processing operations concern the modes in which personal data is provided to internal and external stakeholders. Therefore, the nature of the respective processing operations all concern how personal data is transmitted. The data subjects and the personal data that is processed in these processing operations are also closely linked. Personal data transmitted on the NCCIS may be used when transmitting personal data internally by email and when transmitting personal data externally using post and email. Tusla submitted that when drafting letters, the data

subject's address can be copied from the NCCIS. Furthermore, letters and emails issued internally and externally may also be recorded on the NCCIS. Therefore, the same data subjects and the same personal data may be subject to these different processing operations at the same time and for the same purpose. This illustrates the close link between the processing operations.

9.51 Tusla's infringement of Article 32(1) regarding its failure to implement a process for regularly testing the effectiveness of its *"Records Management Policy"* and *"Information Classification and Handling Policy"* concerns the same processing operations as those concerning Tusla's transmission of personal data. The policies implemented measures for the secure storage and transfer of personal data, for example, the requirement for sensitive information to be sent by encrypted email. Although these policies alone are insufficient to secure these processing operations, the technical and organisational measures contained in the policies directly relate to Tusla's processing operations concerning the transmission of personal data. Therefore, the failure to implement a process for testing the policies also concerns these same processing operations. It follows that this infringement of Article 32(1), (the testing infringement), concerns the same processing operations as the infringements of article 32(1) regarding Tusla's transmission of personal data.

9.52 Regarding Tusla's infringements of Article 33(1), the underlying personal data breaches concerning those infringements relate to the same processing operations that are subject to the findings of infringements of Article 32(1) in this Decision, save in relation to BN-18-9-480, which concerned redaction operations subject to Decision IN-19-10-1. The personal data breach in BN-18-8-146 concerned the security measures for Tusla's transmission of personal data internally by email. The personal data breaches in BN-18-11-74, BN-18-7-303, BN-18-9-156, BN-18-6-288, BN-18-8-244 concerned the security measures for Tusla's transmission of personal data externally by post and email. The personal data breach in BN-18-6-482 concerned the process for regularly testing the effectiveness of Tusla's *"Records Management"* and *"Information Classification and Handling Policy"*. It follows that these infringements of Article 33(1) relate to the same processing operations as the infringements of Article 32(1).

9.53 In light of the above, I am satisfied that the 4 infringements of Article 32(1) found at parts 8(A), (B), (C) and (E) of this Decision concern the same or linked processing operations. Furthermore, I am satisfied that the personal data breaches underlying the infringements of Article 33(1) identified at Part 8(G) of this Decision also concern the same processing operations as those infringements of Article 32(1). Therefore, in deciding the amount of the fine which is to be imposed in respect of these 12 infringements, the total amount of the fine must not exceed the amount specified for the gravest infringement. I consider that Tusla's infringement of Article 32(1) regarding the level of security appropriate to its internal transmission of personal data on the NCCIS is the gravest such infringement. This infringement concerns a huge quantity of highly sensitive personal data transmitted on an internal database that is accessible to thousands of Tusla's staff members. This infringement is most grave and has the potential to cause significant damage to the large number of data subjects in the absence of an appropriate level of security.

9.54 Regarding Tusla's infringement of Article 32(1) in respect of its printing and scanning processing operation, this processing operation is not linked to the processing operations concerning Tusla's transmission of personal data or any of the infringements of Article 33(1). In order to establish that processing operations are linked, within the meaning of Article 83(3), there must be a close nexus between those operations, for example through a common purpose and common nature of processing. The purpose of Tusla's printing and scanning contrasts with the purpose of the processing operations concerning Tusla's transmission of personal data. The purpose is to create softcopy and hardcopy versions of existing documents. Although the transmission of such documents may occur subsequent to such printing and scanning in some instances, this is not sufficient to link the processing operations under Article 83(3). BN-18-8-536 illustrates that this purpose is significantly broader. In that personal data breach, a Tusla staff member scanned a document intending to send it to themselves, resulting in the unintended external transmission of same. This fell outside the purpose of the processing operation. Therefore, it is clear that the purposes of these processing operations are not aligned. Furthermore, the nature of the printing and scanning operations is also distinguished. The nature of this operation concerns the modes for making copies of existing documents. The transmission of personal data between persons is not inherent to this processing operation. Consequently, this processing operation is not linked to the processing operations subject to other findings of infringements. It follows that the administrative fine for this infringement is not limited by reference to other infringements.

iii. Calculating the Administrative Fines

9.55 As outlined above, having carefully considered the infringements, identified in this Decision, the corrective powers that I have decided to exercise in accordance with Section 115 of the 2018 Act and Article 58(2) of the GDPR include the imposition of 2 administrative fines on Tusla:

a. The first administrative fine is imposed in respect of the 12 infringements of articles 32(1) and 33(1), all of which concern the same or linked processing operations. The figure for this administrative fine is calculated with regard to Tusla's infringement of Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its internal transmission of personal data on the NCCIS.

b. The second administrative fine is imposed in respect of Tusla's infringement of Article 32(1) of the GDPR by failing to implement appropriate technical measures to ensure a level of security appropriate to the risk presented by its printing and scanning processing operation.

9.56 The weight to be given to the factors in Article 83(2)(a) to (k) and their impact on the amount of the fines 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[26].

9.57 The methodology that I have followed in calculating the administrative fines is as follows. The first step in calculating each 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 each fine where applicable. Finally, in accordance with Article 83(1) of the GDPR, it is necessary to consider whether the figures arrived at are effective, proportionate and dissuasive in the circumstances. The Draft Decision set out proposed ranges for the administrative fines and the factors to be considered, and the methodology to be used when calculating the fines, in order to provide Tusla with the opportunity comment in accordance with fair procedures. I have had regard to Tusla's submissions on the Draft Decision when calculating the administrative fines.

a. The Infringement of Article 32(1) Concerning Transmitting Personal Data on the NCCIS

9.58 As outlined above when calculating the administrative fine in respect of the infringements of Articles 32(1) and 33(1) for the linked processing operations, I am obliged to ensure that the total amount of that fine does not exceed the amount specified for the gravest infringement. Therefore, in calculating the administrative fine, I shall only have regard to the infringement of Article 32(1) concerning transmitting personal data on the NCCIS because this is the gravest infringement. The other infringements of Article 32(1) and 33(1) are not considered aggravating for the purposes of calculating the fine.

9.59 The permitted range for this administrative fine is set out in Section 141(4) of the 2018 Act [27]. The fine shall not exceed €1,000,000 because Tusla is a public authority[28] that does not act as an *"undertaking"* within the meaning of the Competition Act 2002[29]. 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 **€200,000**

[26] 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.

[27] 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."

[28] 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.

[29] 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.

reflects the seriousness of this infringement and the aggravating factors. This figure is intended to reflect, in particular, the nature of the failure to implement appropriate technical and organisational measures, in accordance with Article 83(2)(a), and in particular how the infringement concerns a database that transmits a huge quantity of highly sensitive personal data to thousands of Tusla staff. I have also had regard to the serious gravity of the infringement pursuant to Article 83(2)(a). Personal data breaches flowing from the infringement have significant capacity to cause material and non-material damage to data subjects. This infringement resulted in BN-18-11-166, which likely resulted in a high level of damage to the data subject. The figure also reflects the fact that the categories of personal data that were not protected by appropriate security measures are particularly sensitive, as considered in accordance Article 83(2)(g) detailed above.

9.60 I consider that the mitigating factors warrant a significant reduction in this fine. Specifically, I consider the factors identified above under Articles 83(2)(b), 83(2)(e), 83(2)(f), and 83(2)(k) of the GDPR mitigating. To take account for the unintentional character of the infringement, I have reduced the fine by **€20,000** in accordance with Article 83(2)(b). 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, in particular the comprehensive plans that address the infringements found in this Decision submitted during the Inquiry and following the Draft Decision, I have reduced the figure by **€60,000** in accordance with Article 83(2)(f). To account for the previous fines imposed on Tusla, I have reduced the figure by **€55,000** in accordance with Article 83(2)(k). Thus, the total figure for reducing the fine in light of the mitigating factors is **€150,000**.

9.61 Applying the mitigating factors, the figure for this administrative fine is **€50,000**. I have considered this 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. As decision-maker for the Commission, I consider it important to strongly discourage non-compliance with the obligation to implement appropriate security measures, particularly with regard to the nature of processing concerned in the NCCIS. 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 **€50,000** meets the requirements of effectiveness, proportionality and dissuasiveness in respect of the infringement and data controller in issue. This amounts to 0.0066% of Tusla's operational budget, or 5% of the cap available.

b. The infringement of Article 32(1) Concerning Tusla's Printing and Scanning Processing Operation

9.62 The permitted range for this administrative fine is also set out in Section 141(4) of the 2018 Act and shall not exceed €1,000,000 for the same reasons as outlined above. Taking into account the seriousness of this infringement and the aggravating factors, the infringement must also be located on this scale of zero to €1,000,000. I consider that the figure of **€125,000** reflects the seriousness of this infringement and the aggravating factors. This figure is intended to reflect, in particular, the serious nature and the gravity of the infringement. The infringement has the potential to cause a high level of damage, which is reflected in the scanning disclosure in BN-18-8-536, whereby special category personal data was disclosed to an external recipient. Pursuant to Article 83(2)(g), I have also had regard to the high sensitivity of the categories of personal data concerned in the infringement.

9.63 I also consider that the mitigating factors in relation to this infringement warrant a significant reduction in this fine. Specifically, I consider the factors identified above under Articles 83(2)(b), 83(2)(c), 83(2)(e), 83(2)(f), and 83(2)(k) of the GDPR mitigating. To take account for the unintentional character of the infringement, I have reduced the fine by **€7,500** in accordance with Article 83(2)(b). To account for the action taken by Tusla to mitigate the damage suffered by data subjects in BN-18-8-536, BN-18-6-584 and BN-18-8-184, I have reduced the fine by **€12,500** in accordance with Article 83(2)(c). To account for the lack of relevant previous infringements by Tusla, I have reduced the figure by **€5,000** in accordance with Article 83(2)(e). To account for the cooperation that Tusla engaged with the DPC to remedy the infringement, in particular the plan submitted to fully implement organisation-wide secure print and scan facilities by 30th September 2021, I have reduced the figure by **€30,000** in accordance with Article 83(2)(f). To account for the previous fines imposed on Tusla, I have reduced the figure by **€35,000** in accordance with Article 83(2)(k). Thus, the total figure for reducing the fine in light of the mitigating factors is **€90,000**.

9.64 Applying the mitigating factors, the figure for the administrative fine is **€35,000**. I have considered this proposed range in light of the requirement in Article 83(1) that administrative fines shall be "effective, proportionate and dissuasive". As outlined above, I consider it important to strongly discourage non-compliance with the obligation to implement appropriate security measures. This is also the case with regard to the broad scope of Tusla's printing and scanning processing operation. I consider that the figure of **€35,000** meets the requirements of effectiveness, proportionality and dissuasiveness in respect of the infringement and data controller in issue. This amounts to 0.0046% of Tusla's operational budget, or 3.5% of the cap available.

iv. Summary: Administrative Fines

9.65 In summary, this Decision imposes two administrative fines in respect of the infringements of articles 32(1) and 33(1) that have been identified herein. The final figures for those fines is as follows:

Fine 1: €50,000 (infringement of Article 32(1) concerning transmitting personal data on the NCCIS).
Fine 2: €35,000 (infringement of Article 32(1) concerning Tusla's Printing and Scanning Processing Operation).

9.66 Therefore, the total of the fines imposed in this Decision is **€85,000**.

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. Furthermore, in circumstances where this Decision includes decisions to impose two administrative fines, pursuant to Section 142 of the 2018 Act, Tusla also has the right to appeal against the decisions to impose administrative fines within 28 days from the date on which notice of the decisions is given to it.

Helen Dixon
Commissioner for Data Protection

Appendix: Personal Data Breaches Considered in the Inquiry

As outlined above, in accordance with Section 111(1) of the 2018 Act, this Decision considers all the information obtained in the Inquiry in making findings as to whether infringements of the GDPR and/or the 2018 Act have occurred or are occurring. The information considered includes, but is not limited to, the 71 personal data breach notifications submitted by Tusla. While it does not necessarily follow from a controller's notification of a personal data breach that the breach was caused by an infringement of the GDPR or the 2018 Act, the personal data breach notifications are illustrative of how Tusla transmits personal and updates personal data, and, in some instances, of technical and organisational measures implemented at the time of the breaches. Therefore, the table in this appendix provides a summary of this Decision's consideration of the 71 personal data breach notifications; including the part of the Decision that each personal data breach notification is relevant to; and the thematic topic arising.

Number	Breach Notification Reference	Part	Thematic Topics
1	BN-18-6-18	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
2	BN-18-6-40	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
3	BN-18-6-41	Part 3 – Pre-GDPR	N/A
4	BN-18-6-53	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
5	BN-18-6-123	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
6	BN-18-6-191	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
7	BN-18-6-227	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
8	BN-18-6-239	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
9	BN-18-6-250	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
10	BN-18-6-252	Part 3 – Pre-GDPR	N/A
11	BN-18-6-285	Part 3 – Pre-GDPR	N/A
12	BN-18-6-288	Part 8(C) – Transmitting Personal Data Externally and 8(G) Duty to Notify Personal Data Breaches	Security of Processing and Notifications of Personal Data Breaches
13	BN-18-6-299	Part 3 – Pre-GDPR	N/A
14	BN-18-6-316	Part 8(C) – Transmitting Personal Data Externally	Security of Processing

15	BN-18-6-379	Part 3 – the relevant issues were considered in another decision of the DPC (Decision IN-19-10-1)	N/A
16	BN-18-6-411	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
17	BN-18-6-482	Part 8(E) - Processes for Testing Security Measures and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing and Notifications of Personal Data Breaches
18	BN-18-6-483	Article 8(G) - Duty to Notify Personal Data Breaches	Notifications of Personal Data Breaches
19	BN-18-6-484	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
20	BN-18-6-534	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
21	BN-18-6-549	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
22	BN-18-6-584	Part 8(D) – Printing and Scanning	Security of Processing
23	BN-18-6-571	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
24	BN-18-7-124	Part 8(E) - Processes for Testing Security Measures	Security of Processing
25	BN-18-7-236	Part 3 – Pre-GDPR	N/A
26	BN-18-7-266	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
27	BN-18-7-303	Part 8(C) – Transmitting Personal Data Externally and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing and Notifications of Personal Data Breaches
28	BN-18-7-322	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
29	BN-18-7-471	Part 8(E) - Processes for Testing Security Measures	Security of Processing
30	BN-18-7-479	Part 3 – Pre-GDPR	N/A
31	BN-18-7-602	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
32	BN-18-7-603	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
33	BN-18-8-29	Part 8(E) - Processes for Testing Security Measures	Security of Processing
34	BN-18-8-120	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
35	BN-18-8-146	Part 8(B) – Transmitting Personal Data Internally by Email and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing and Notifications of Personal Data Breaches
36	BN-18-8-184	Part 8(D) – Printing and Scanning	Security of Processing
37	BN-18-8-209	Part 3 – Pre-GDPR	N/A

38	BN-18-8-236	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
39	BN-18-8-244	Part 8(C) – Transmitting Personal Data Externally and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing and Notifications of Personal Data Breaches
40	BN-18-8-297	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
41	BN-18-8-315	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
42	BN-18-8-316	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
43	BN-18-8-333	Part 8(C) – Transmitting Personal Data Externally and Part 8(F) - Data Accuracy	Security of Processing and Personal Data Accuracy
44	BN-18-8-338	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
45	BN-18-8-339	Part 8(B) – Transmitting Personal Data Internally by Email	Security of Processing
46	BN-18-8-416	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
47	BN-18-8-454	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
48	BN-18-8-476	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
49	BN-18-8-519	Part 8(C) – Transmitting Personal Data Externally and Part 8(F) - Data Accuracy and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing, Personal Data Accuracy, and Notifications of Personal Data Breaches
50	BN-18-8-536	Part 8(D) – Printing and Scanning	Security of Processing
51	BN-18-8-554	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
52	BN-18-9-43	Part 8(E) - Processes for Testing Security Measures	Security of Processing
53	BN-18-9-57	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
54	BN-18-9-156	Part 8(C) – Transmitting Personal Data Externally and Part 8(F) - Data Accuracy and Article 8(G) - Duty to Notify Personal Data Breaches	Security of Processing, Personal Data Accuracy and Notifications of Personal Data Breaches
55	BN-18-9-246	Part 3 – Pre-GDPR	N/A
56	BN-18-9-249	Part 3 – the relevant issues were considered in another decision of the DPC (Decision IN-19-10-1)	N/A
57	BN-18-9-289	Part 8(C) – Transmitting Personal Data Externally	Security of Processing

58	BN-18-9-345	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
59	BN-18-9-400	Part 3 – the relevant issues were considered in another decision of the DPC (Decision IN-19-10-1)	N/A
60	BN-18-9-480	Part 3 – the relevant issues were considered in another decision of the DPC (Decision IN-19-10-1)	N/A
61	BN-18-10-18	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
62	BN-10-10-115	Part 8(E) - Processes for Testing Security Measures	Security of Processing
63	BN-18-10-194	Part 3 – Pre-GDPR	N/A
64	BN-18-10-402	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
65	BN-18-10-439	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
66	BN-18-11-73	Part 8(H) – information obtained is not probative in relation to whether an infringement occurred	N/A
67	BN-18-11-74	Part 8(C) – Transmitting Personal Data Externally and Part 8(F) - Data Accuracy and Article 8(G) - Duty to Notify Personal Data Breaches	Personal Data Accuracy and Notifications of Personal Data Breaches
68	BN-18-11-75	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
69	BN-18-11-158	Part 8(C) – Transmitting Personal Data Externally	Security of Processing
70	BN-18-11-166	Part 8(A) – Transmitting Persona Data on the NCCIS	Security of Processing
71	BN-18-11-209	Part 3 – Pre-GDPR	N/A