In the matter of the General Data Protection Regulation

DPC Case Reference: IN-20-4-8

In the matter of [redacted]

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

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

DECISION

Decision-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

24 January 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction 3
2. Legal Framework for the Inquiry and the Decision 3
   i. Legal Basis for the Inquiry 3
   ii. Legal Basis for the Decision 4
3. Factual Background 4
4. Findings 6
   i. Risk Assessment 8
   ii. Findings 11
5. Decision on Corrective Measures 11
6. Right of Appeal 14

Appendix: Schedule of Materials Considered for the Purposes of this Decision 15

1. Introduction

1.1 This document ("**the Decision**") is a Decision of the Data Protection Commission ("**the DPC**") in accordance with Section 111 of the Data Protection Act (**"the 2018 Act").** I make this Decision having considered the information obtained in the own volition inquiry (**"the Inquiry"**) conducted by a Case Officer of the DPC (**"the Case Officer")** pursuant to Section 110 of the 2018 Act. The Case Officer who conducted the Inquiry provided [redacted] with the Draft Inquiry Report and the Final Inquiry Report. The Decision is being provided to [redacted] pursuant to Section 116(1)(a) of the 2018 Act in order to give [redacted] 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.

1.3 [redacted] was provided with the Draft Decision on this inquiry on 30 November 2021 to give it a final opportunity to make submissions. [redacted] acknowledged receipt of the Draft Decision on 14 December and made submissions to which I have had regard in coming to my decision.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

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

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

ii. Legal Basis for the Decision

2.3 The decision-making process for this Inquiry is provided for under Section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the proposed corrective powers, if any, to be exercised. As the sole member of the Commission, I perform this function in my role as the Decision-Maker in the DPC. In so doing, I am required to carry out an independent assessment of all the materials provided to me by the Case Officer as well as any other materials that the Council has furnished to me and any other materials that I consider relevant, in the course of the decision-making process.

2.4 The Final Inquiry Report was transmitted to me on 21 January 2021, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and [redacted] and copies of all submissions made by [redacted] including the submissions made by [redacted] in respect of the Draft Inquiry Report. [redacted] made submissions on the Draft Decision on 14 December 2021. A full schedule of all documentation considered by me for the purpose of this Decision is appended hereto. I issued a letter to [redacted] on 04 October 2021 to notify it of the commencement of the decision-making process.

2.5 Having reviewed the Final Inquiry Report, and the other materials provided to me by the Case Officer, including the submissions made by [redacted] I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout. This includes, but is not limited to, notifications to [redacted] and opportunities for [redacted] to comment on the Draft Inquiry Report before the Case Officer transmitted it to me as decision-maker.

3. Factual Background

3.1 [redacted] is an employee relations consultancy firm that was engaged by the Personal Injuries Assessment Board ("**PIAB**") to carry out an investigation into [redacted]. The relationship between the parties was governed by a Consultancy Agreement, entered into on 07 May 2019. In addition, Terms of Reference were agreed between the parties which set out the investigative process to be to be carried out by [redacted]

3.2 The Terms of Reference outline that on completion of the investigation process, [redacted] must provide a report to PIAB, stating:

"The Reviewer[1] will thereafter, prepare a written report which will include details of [redacted], the response of the Respondent, any findings of fact, including a finding as to [redacted], and make recommendations, if appropriate, on any action required…The Reviewer's final report will issue to [redacted], PIAB."

3.3 On 24 September 2019, [redacted] emailed asking if PIAB had received the electronic appendices relating to the six investigation reports. The email also asked, if they had not been sent on, to whom they should be sent. It should be noted at this stage that this personal data had already been provided in hard copy to PIAB on 01 October 2019.

3.4 On 26 September 2019, the PIAB responded to [redacted] by email stating that it had the final reports:

"which is what was required and in line with the terms of reference."

The email went on to state:

"We do not require e-appendices or any further documentation to be forwarded to us."

3.5 In its submissions to the DPC dated 01 November 2021, [redacted] stated that it was of that view that, had it adhered to PIAB's instruction i.e. not sent the personal data, of which PIAB already had a copy, to PIAB,

"…[this would] have left the PIAB exposed to accusations of non-compliance with [redacted] requirements, because the PIAB would not be in possession of the complete investigation report (inclusive of appendices)".

3.6 On 28 November 2019, [redacted] sent a letter to the PIAB containing a USB storage device. The letter stated

"Please see the USB appended to this letter for the appendices related to the 6 [redacted] that [redacted] conducted on behalf of PIAB."

3.7 When delivered, the USB storage device was missing from the envelope received by the PIAB and the envelope in which the letter was placed had suffered some damage. The USB storage device was neither encrypted nor password protected. [redacted] has acknowledged that registered post was not used in this instance. Nor has it been claimed that a secure envelope, such as a padded envelope, was used to assist in securing the safe delivery of the unencrypted device.

[1] "The Reviewer" is defined as "[redacted] in the Terms of Reference.

3.8 The DPC received notification of a National Breach from PIAB on 10 December 2019 under breach notification [redacted]. Following an examination of the breach notification, the DPC was of the opinion that one or more provisions of the 2018 Act and/or the GDPR may have been contravened in relation to the personal data of data subjects in respect of which [redacted] is the data controller/data processor for the purposes of the Act and the GDPR.

3.9 In reviewing the matters raised in the breach report, the DPC considered it appropriate to establish a full set of facts so that it could assess whether or not [redacted] had discharged its obligations as data controller/data processor in connection with the subject matter of the breach and determine whether or not any provision(s) of the Act and/or the GDPR had been contravened by [redacted] in that context.

3.10 Accordingly, the DPC took the decision to conduct an Inquiry on its own volition into the suspected infringements.

3.11 [redacted] was provided with the Draft Decision in this inquiry on 30 November 2021 to give it a final opportunity to make submissions. I received submissions from [redacted] on 14 December, in addition to submissions made by [redacted] in advance of the Draft Decision being furnished to it, received by the DPC on 01 November 2021 and on 16 November 2021. I have given consideration to these submissions in advance of arriving at a final Decision. This Decision is being provided to [redacted] pursuant to sections 116(1)(a) and 126(a) of the 2018 Act in order to give [redacted] notice of the Decision, the reasons for it and the corrective powers that I have decided to exercise.

3.12 This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the GDPR arising from the infringements which have been identified herein by the Decision Maker.

4. Findings

4.1 Following intensive examination of the facts in this case, including a review of the Draft and Final Inquiry Report, the Draft Decision and the submissions made by [redacted] and given that PIAB had directed in advance of the posting of the USB storage device by [redacted] that no further personal data be sent to it, as set out in paragraphs 3.3 and 3.4 above, I find that the material issues in this inquiry net down to one central issue : the security of processing under Article 32(1) undertaken by [redacted] in electing to post the USB in the manner carried out, to PIAB.

4.2 Article 32 of the GDPR sets down obligations for both controllers and processors. In subsection (1) it requires that :

> *"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."

4.3 Article 32(1) GDPR obliges controllers and processors, in processing personal data, to implement a level of security appropriate to the risk presented to the rights and freedoms of natural persons. The level of security must have regard to 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. This Decision considers the appropriateness of the security measures implemented by [redacted] in respect of the processing of personal data by saving to the USB storage device and sending by post in the manner in which it was sent.

4.4 Article 32(1) provides a non-exhaustive list of such measures which may be taken to implement an appropriate level of security, which may include, as appropriate, pseudonymisation and encryption of personal data, the ability to ensure on-going confidentiality of processing systems, the ability to restore access to personal data in the event of an incident, and a process for regularly testing and assessing the effectiveness of technical and organisational measures for ensuring security of processing.

4.5 In considering whether the requirements of Article 32 have been met by the controller and/or processor, it is necessary to assess whether the controller and/or processor has adequately gauged the level of risks to data subjects and whether the controller and/or processor has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The different factors listed in Article 32(1) should be taken into account when carrying out this assessment. If a controller and/or processor has correctly identified the risks and has implemented appropriate security measures there will be no infringement of Article 32 of the GDPR, even in the event of a personal data breach. However, in practice, many personal data breaches occur as a result of a lack of appropriate technical and organisational measures in place.

4.6 In the DPC's Letter of Notice of the Commencement of an Inquiry to [redacted] dated 08 May 2020 ("**the Commencement Letter**") the Case Officer sought that [redacted]

provide additional specific information in regard the measures in place, at the time of the breach, to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR in terms of:

a. An assessment of the risks of varying likelihood and severity associated with the forms of data processing at issue in the breaches

b. Appropriate technical and organisational measures to counter those risks

c. Capability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

d. Processes for regular testing, assessment and evaluating the effectiveness of the technical and organisation measures for ensuring the security of the processing

i. Risk Assessment

a. An assessment of the risks of varying likelihood and severity associated with the forms of data processing at issue in the breaches

4.7 The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the processing. Article 32(2) of the GDPR expressly states that the risks of loss, alteration, unauthorised disclosure or access to the personal data should be considered when assessing the appropriate level of security. Regarding [redacted] processing of personal data, these risks include a loss of the relevant information contained within their investigative reports (including the appendices), as well as a risk of that information being accessed by an unauthorised third party, it being altered or deleted or shared.

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

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

4.8 It is necessary to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. In [redacted] case, this risk assessment must have particular regard to ensuring the integrity and accuracy of personal data in the investigative reports. The risk assessment should also have particular regard to the risk of unauthorised disclosure to third parties.

4.9 Regarding the nature, scope, context and purposes of [redacted] processing of personal data, as outlined above, the nature of [redacted] processing is sensitive. Its scope in the specific case of the personal data breach is limited to approximately 18 individuals' personal data. The context for sharing the data arises in relation to its work on [redacted]. The purpose of the processing is to provide copies of completed reports regarding [redacted] to its client.

4.10 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[2] provides guidance as to the factors that should inform this risk assessment. In this case the CJEU declared the Data Retention Directive to be 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. In assessing the risk posed by [redacted] processing, regard must also be had to these factors.

4.11 In its reply to the Commencement Letter, [redacted] stated that it considered the risks in processing the data as follows:

> *"1. Staff awareness of the issues and failure to abide by organisational requirements (detailed below)*
>
> *2. General IT issues, including security and compliance generally (detailed below)*
>
> *3. Encryption of the data being transferred as appropriate (detailed below)*
>
> *4. Postage (detailed below)"*
>
> *c. See b. above*
>
> *d. See b. above. These processes were regularly considered and this is evidenced by the pro-active steps taken prior to GDPR in ensuring the systems were compliant. Our DP arrangements were also considered in May 2019 and that documentation is attached in Appendix 2. Finally, in relation to the transmission of reports in particular, this was considered on a case by case basis and was therefore discussed at team case reviews."*

4.12 I find that [redacted] processing of personal data regarding its [redacted] reports gave rise to a moderate risk to the data subjects' fundamental rights and freedoms. In coming to this finding, I have had particular regard to the nature of the personal data processed in such investigations and the context of that processing.

[2] 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).

b. Appropriate technical and organisational measures to counter those risks

4.13 In its reply to the Commencement Letter, [redacted] stated that the following technical and organisational measures were in place to counter the risks to the fundamental rights and freedoms of data subjects that processing presented:

"1. Staff training, with particular emphasis on induction and persistent reference to DP issues at daily case review meetings and weekly planning meetings. This was supported by extensive well-defined business steps for all of our processes assisted by checklists designed to comply with all [redacted] constraints. The employee responsible for the breach was brought through induction on 22 November 2019. This matter contributed to her employment being terminated on 18 December 2019 indicating how seriously these matters are considered within [redacted] also has contractual requirements to ensure confidentiality continues after the employment ends and that while errors are a natural phenomenon, a knowing failure to notify of any issue will be considered gross misconduct.

2. This was reviewed in advance of the coming into force of GDPR and following this review it was necessary to remove our cloud storage from the supplier Dropbox as it was not able to satisfy [redacted] that data would be held within the EU. [redacted] migrated to Google Drive and the relevant Agreement is available if required. All of our laptops and tablets are encrypted. We use Apple products so that we can also avail of the remote wiping. All of these are deliberate choices made in an effort to ensure the security of data we process.

3. All substantive information transferred between [redacted] and PIAB employees by email was done by encrypted PDF by email. This is our standard practice. Reports with appendices are normally too large to be sent as an encrypted PDF by email. It was also our understanding that a USB device encrypted on an iMac, as used by [redacted] cannot be opened by a Windows device which creates an accessibility issue for the vast majority of our clients. This has been incorporated into the IT review underway for verification and solution.

4. It was a rule within [redacted] that anything sent by post was to be sent by registered post. In particular, it was [redacted] understanding that envelopes sent by registered post were not subject to the same machine sorting as standard mail."

4.14 Regarding processes for regular testing, assessment and evaluating the effectiveness of the technical and organisation measures for ensuring the security of the processing [redacted] submitted:

"d. See b. above. These processes were regularly considered and this is evidenced by the pro-active steps taken prior to GDPR in ensuring the systems were compliant. Our DP arrangements were also considered in May 2019 and that documentation is attached in Appendix 2. Finally, in relation to the transmission of reports in particular, this was considered on a case by case basis and was therefore discussed at team case reviews."

4.15 Despite registered post being cited by [redacted] as an organisational measure to counter the risks, the envelope in this case was sent by ordinary post.

4.16 I note that [redacted] states that an encrypted pdf was too large to send by email. However there is no explanation given to describe why an encrypted pdf was not placed on the USB storage device.

4.17 There is a distinction to be made between encryption of an entire device (which may cause difficulties for a different Operating System) and encryption of the files contained within a device. The possibility of a Windows machine reading a file that had been encrypted using an iMac is dependent on the encryption method used. For example, PGP encrypted files (using GPG Suite or another tool) on a USB storage device formatted to exFAT are readable on Windows/Linux/Mac. It is also possible to use an IOS tool like Keka to produce a .7z file that behaves exactly like 7zip, including AES 256 encryption (so that it could be placed on a USB storage device or emailed) and volume spanning, which would allow the encrypted material to be sent by email.

4.18 Further, it is unclear why Google Drive was not considered as a secure means of transferring the data, given that it was in place as part of [redacted] preparedness for the coming in to effect of the GDPR in May 2018. Use of Google Drive could be considered a technical measure which would have lessened the risk of loss or damage to the personal data in transferring it to PIAB.

4.19 I consider that the security measures for the protection of personal data in place at the time of the breach were not appropriate in respect of the moderate risk of the processing. There were a variety of technical measures which could have been used to securely transfer the data and minimise the risk that the data would be lost or otherwise manipulated in an unauthorised manner. Such measures include the use of a padded envelope, the use of Google Drive, or the encryption of the files stored upon the USB storage device. In the circumstances outlined above, I find that the measures implemented by [redacted] were not appropriate to ensure a level of security appropriate to the risk.

ii. Findings

4.20 Having reviewed the Draft and Final Inquiry Reports and [redacted] submissions, I find that [redacted] infringed Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data.

5. Decision on Corrective Measures

5.1 I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that [redacted] has infringed Article 32(1) GDPR. Under section 111(2) of the 2018 Act I must now make a decision as to whether corrective powers should be exercised in respect of [redacted] and if so, the corrective powers to be exercised. The remaining question for determination in this Decision is whether or not those findings merit the exercise of any of the corrective powers set out in Article 58(2) GDPR, and if so, which one(s).

5.2 Recital 129, which acts as an aid to the interpretation of Article 58 provides that

> *"…each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…"*

5.3 In the circumstances of the within inquiry and the findings of infringement, I find that the exercise of one or more corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR. Having carefully considered the infringement identified in this Decision, I have decided to exercise corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) 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 power set out in Article 58(2). In summary the corrective powers that I have decided to exercise are:

a) Article 58(2)(b) – I have decided to issue a reprimand to [redacted] in respect of its infringement of Article 32(1) GDPR.

5.4 Having identified that [redacted] has infringed Article 32(1), I am obliged to consider what corrective measures are necessary. In this case, [redacted] has already notified the DPC and provided detail of the changes it is instituting to its processes in order to secure personal data in any similar scenario arising in the future.
In its submissions dated 01 November, [redacted] stated that since the breach incident it has retained the services of data security consultants and enhanced its practices further to the recommendations of those consultants, noting,

> *"…[redacted] has since that time learned more about encryption technology and has applied that learning to enhance its processes."*

5.5 It further stated that since the breach incident it had undertaken had undertaken actions to "enhance its compliance with its GDPR obligations", these being:

> *"(a) hired a forensic data security consultancy to complete a forensic security review, and implemented the recommendations of that review;*
>
> *(b) changed its IT system to a system that facilitates a greater level of security;*

(c) now applies encryption to all electronic files containing personal data that are provided by [redacted] to its clients;

(d) applies enhanced data protection procedures, including by the introduction of a more comprehensive suits of data protection policies and procedures than previously were in place (these are provided in the appendices of the Final Inquiry Report0; and

(e) provides enhanced training for its staff as well as continuing the daily discussion of how to ensure compliance in respect of individual cases on which [redacted] is working For example, two of [redacted] four employees successfully completed, in May 2021, a professional post-graduate diploma in data protection, run by the Kings Inns."

5.6 I welcome these submissions that improved security and organisational measures have been put in place. As a result, I do not consider it necessary in this case to issue an order requiring processing to be brought into compliance.

5.7 In its submissions dated 14 December 2021, [redacted] considered that a reprimand in this case did not constitute a "mild sanction" and further stated (in relation to its objection to the provisional levying of a reprimand in my Draft Decision to ensure future compliance with the infringed Articles of the GDPR),

"A reprimand is unnecessary for that purpose because [redacted] has already achieved compliance in the present, rather than in the future."

5.8 However, recital 148 to the GPDR, while not an operative part of the law but nonetheless persuasive in interpreting provisions of the GDPR, proposes that in a case of a minor infringement a reprimand may be issued instead of a fine. This is the case regardless of whether corrective or mitigation actions have since been implemented.

5.9 I issue [redacted] a reprimand in respect of its infringement of Article 32(1) GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to "issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation". Each measure that I impose by way of the exercise of a corrective power for the infringement I have found must be appropriate, necessary and proportionate in view of ensuring compliance with the GDPR. In this respect, I consider it appropriate, necessary and proportionate to impose a reprimand without the additional corrective measure of a fine in order to give full effect to the obligations in Article 32 and to formally recognise the infringement found in this Decision, having particular regard to the how [redacted] processing of personal data regarding its [redacted] reports gives rise to a moderate risk to the data subjects' fundamental rights and freedoms.

5.10 I am also obliged to consider whether a fine in addition to any other measure should be imposed in this case. I have set out above how [redacted] processing regarding its investigative reports creates a moderate risk to data subjects. In determining whether to impose an administrative fine, I must have regard to, amongst other things, the level of

damage suffered by data subjects. In this regard, I must consider the level of risk caused by the personal data breach in the circumstances, as distinct from the level of risk caused by [redacted] processing of personal data. I consider the personal data breach in this case caused a low to moderate risk of damage to data subjects. I consider that the risk of damage to the data subjects was low to moderate because if the unencrypted USB key were found by a member of the public and the data accessed, it is of very limited use. In light of the fact that a very limited number of data subjects could be impacted, and the relatively low risk of damage in the case, I do not consider it appropriate to impose an administrative fine.

6. Right of Appeal

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

Helen Dixon
Commissioner for Data Protection

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

The Case Officer delivered the Final Inquiry Report to me on 21 January 2021. I also had regard to all of the correspondence, submissions, and documentation gathered during the Inquiry and the decision-making stage, including:

1. [redacted] web page extract (19 June 2020)
2. Commencement Letter
3. Documentation for BN-19-12-226
4. Breach Notification from the PIAB
5. Email DPC to [redacted] with questions 23 April 2020
6. Email [redacted] to DPC response 1 May 2020 and Consultancy Agreement
7. [redacted] Submissions 29 May 2020
8. [redacted] response to Commencement Letter
9. Terms of Reference document
10. Data Protection analysis
11. Template Data Processor contract
12. Data Protection Policy
13. [redacted] complaint to PIAB 03 October 2019
14. Staff statement
15. Dropbox correspondence
16. Interview template

[redacted]

18. Correspondence [redacted] PIAB
19. Relevant documentation provided by the PIAB
20. Emails [redacted] / PIAB 24 and 26 September 2019
21. Letter [redacted] to PIAB 28 November 2019
22. Email requesting information from [redacted]
23. Submissions 27 August 2020
24. [redacted] Submissions 27 August 2020
25. DPC Correspondence 1 October 2020
26. Letter to [redacted] 1 October 2020
27. Terms of Reference (PIAB version)
28. Potential Data Breach Report
29. Email PIAB to [redacted] re issue 10 December 2019
30. Submissions 22 October 2020
31. [redacted] Submissions 22 October 2020

Letters with submissions from [redacted] following commencement of the decision-making stage:

1. Dated 01 November 2021

2. Dated 16 November 2021
3. Dated 14 December 2021