In the matter of the General Data Protection Regulation

DPC Case Reference: IN-18-12-01

In the matter of the Department of Employment Affairs

and Social Protection

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

10 May 2021

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**"the Decision"**) is a decision made by the Data Protection Commission (**"the DPC"**) in accordance with Section 111 of the Data Protection Act 2018 (**"the 2018 Act"**). I make this Decision having considered the information obtained in the separate own volition inquiry (**"the Inquiry"**) conducted by authorised officers of the DPC (**"the Inquiry Team"**) pursuant to Section 110 of the 2018 Act. The Inquiry Team provided the Department of Employment Affairs and Social Protection **("the Department")** with the Draft Inquiry Report and the Final Inquiry Report.

1.2 The Department was provided with the Draft Decision on this Inquiry on 8 March 2021 to give it a final opportunity to make submissions. The Department made submissions on the Draft Decision on 29 March 2021 and I have had regard to those submission before making this Decision. This Decision is being provided to the Department pursuant to Section 116(1)(a) of the 2018 Act in order to give the Department notice of the Decision and the reasons for it.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 The General Data Protection Regulation **("the GDPR")** is a legal regime concerning 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, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

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

ii. 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 corrective powers, if any, to be exercised. As the sole member of the DPC, 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 of the materials provided to me by the Inquiry Team as well as any other materials that the Department 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 11 February 2021, together with the Inquiry Team's file, containing copies of all correspondence exchanged between the Inquiry Team and the Department; and copies of all submissions made by the Department, including the submissions made by the Department in respect of the Draft Inquiry Report. The Department made submissions on the Draft Decision on 29 March 2021. A full schedule of all documentation considered by me for the purpose of this Decision is appended hereto. I issued a letter to the Department on 12 February 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 Inquiry Team, including the submissions made by the Department, 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 the controller, the voluntary interview conducted, and opportunities for the controller to comment on the Draft Inquiry Report before the Inquiry Team submitted it to me as decision-maker.

3. Factual Background

3.1 The Department is a Government department that processes high volumes of personal data of almost all persons in Ireland, including in the context of making social welfare payments. In that context, the Department has statutory responsibility for the issuing of Personal Public Service Numbers to individuals and in some cases Public Services Cards. This Inquiry concerns the process leading to the amendment of the Department's *"Privacy Statement"* (**"the Privacy Statement"**) on 6 July 2018. The Privacy Statement details the personal data the Department collects and processes as part of its various personal data processing operations. The Department amended paragraph 3.3 of that statement, which was part of the section titled *"What types of Personal Data do we Collect".* It replaced part of the paragraph that stated that the Department collects *"biometric data"* with a reference to *"data such as photographs"*. The Department also removed an express reference to *"special categories of personal data"*. The original text read as follows:

> *"At times, we also need to collect 'special categories' of personal data such as data concerning health and biometric data used for the purpose of identification and, at times, information concerning trade union membership."*

3.2 The revised text read as follows:

> *"At times, we also need to collect personal data, such as health data and data such as photographs used for the purposes of identification. This may also include information concerning trade union membership."*

3.3 The scope of this Inquiry, as further detailed in Part 4, concerns whether the Department's Data Protection Officer (**"DPO"**) was involved in the issue of amending the Privacy Statement in a proper and timely manner in accordance with Article 38(1) of the GDPR; and whether the DPO received instructions regarding the exercise of his tasks contrary to the requirements of Article 38(3) of the GDPR. Following the Department's amendment, there was no reference to biometric data in any section of the Privacy Statement. Privacy Statements are important tools in assisting organisations to comply with their transparency obligations under the GDPR. However, the question of whether the Department in fact complied with its transparency obligations is outside the scope of this Inquiry.

3.4 The purpose of Article 38(1) of the GDPR is to ensure that the expertise of the DPO is available on all issues that relate to the protection of personal data[1]. The Department amended its Privacy Statement after a significant number of internal emails and discussions between 4 July – 6 July 2018. This inquiry must consider these emails, discussions and the broader context in which the amendment occurred in order to determine whether the DPO was involved in the issue of amending the Privacy Statement in a proper and timely manner. These events are also central to determining whether the DPO received instructions regarding the exercise of his tasks contrary to the requirements of Article 38(3) of the GDPR. Therefore, it is necessary for this Decision to detail the factual background surrounding the emails and discussions that occurred within the Department between 4 - 6 July 2018.

3.5 Prior to the GDPR coming into force on 25 May 2018, there was no requirement in law for organisations to designate a DPO. However, Article 37(1) of the GDPR requires the designation of a DPO in certain circumstances, including where processing of personal data is carried out by public authorities or public bodies. Therefore, the Department was obliged to designate a DPO from when the GDPR came into force on 25 May 2018. Having designated a DPO, the Department was obliged to comply with the requirements of Article 38.

3.6 The Department's submissions on the Draft Inquiry Report stated, *"the Department has at all times openly acknowledged that it processes biometric data."*[2] In doing so, the Department distinguished collecting biometric data with processing biometric data. Those submissions went on to outline how the Department processes biometric data as part of its "SAFE" registration. The SAFE registration is a process used by the Department to register data subjects for Public Services Cards. The Department captures photographs of applicants during this process. The Department's submissions quoted its website in outlining how it processes those photographs:

> *"The Department of Employment Affairs and Social Protection uses facial image matching software to strengthen the SAFE registration process by detecting and deterring duplicate SAFE registration attempts. The normal digital photograph (in JPEG format) captured during the SAFE registration process is input into and stored in*

[1] Article 37(5) GDPR requires that DPOs shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law.
[2] The Department's submissions on the Draft Inquiry Report, dated 24 July 2019, at page 14.

this facial image matching software. It is then modelled and searched against the Department's photo database to ensure that the person in the photograph has not already been registered using a different Personal Public Service Number or a different identity dataset. The software compares photographs by converting the image into an arithmetic template based on the individual's facial characteristics, e.g., distance between their eyes, height of cheekbones etc., and checking it against the other image templates already held in that software's database from other SAFE registrations. A similar approach is taken by the Passport Office in its systems when processing passport applications/renewals. Up to the end of September 2017 the Department had detected some 165 cases of suspected identity fraud as a result of this matching process.

It is important to note that the arithmetic models behind the photographs do not get stored on the PSC or in the Public Service Identity dataset. Consequently, this data is not shared with any other public body. They are only stored in the facial image matching software's database held in the Department's own secure datacentres.

It is also important to note that the Department does not ask for or collect other biometric data from our customers (e.g., fingerprints, retinal scans, etc.) nor does it use advanced facial mapping cameras when taking the photo as part of the SAFE registration process"[3]

3.7 In early May 2018, the Minister for Employment Affairs and Social Protection answered a number of parliamentary questions concerning biometric data. The Department submitted the text of these parliamentary questions to the DPC in the context of responding to a DPC query regarding the content of any advice furnished by the DPO to the Department in relation to the collection and/or processing of biometric data[4]. The Minister stated that Public Services Cards do not store biometric data and that the Department does not ask for or collect biometric data from their customers. In the answers, the Minister also stated that the Department uses facial matching technology. The Minister outlined how the Department converts the images that it collects during the SAFE registration process into an arithmetic template and stores them in facial image matching software held in the Department's data centres. Furthermore, the media query relevant to this Inquiry asked the Department about its position on processing biometric data. Similar to the Minister's answers, the Department's response to the media query stated that Public Services Cards do not store biometric data, and then outlined how the Department uses facial image matching technology, but did not acknowledge that this constitutes the processing of biometric data.

3.8 In its submissions on the Draft Decision, the Department submitted that the approach adopted by the Minister and the Department regarding its comments on biometric data, and the broader context of this approach, is not relevant to the scope of the Inquiry. It is useful

[3] Ibid.

[4] The text of the Parliamentary Questions and answers provided were submitted in the Department's Interim Response to the Data Protection Commission's Inquiry Ref: 18-12-01, dated 19 December 2018.

to address these submissions before proceeding with the factual background in this Decision. The basis for the Department's submission is that the scope of the Inquiry does not consider whether the Department complied with its transparency requirements under the GDPR. For the avoidance of doubt, this Decision does not consider, nor does it make any findings in relation to, the Department's compliance with its transparency obligations under the GDPR. Such matters are outside the scope of the Inquiry. However, the Minister and the Department's positions on biometric data prior to, and at the time of, the amendment to the Privacy Statement are directly relevant to the question of whether the Secretary General gave due weight to the advice of the DPO and the Data Protection Unit as is required in accordance with the requirement of proper involvement under Article 38(1) (as further detailed in part 6 of this Decision).

3.9 The relevance of these positions on biometric data to this Inquiry is best understood in light of how the Secretary General, in deciding to amend the Privacy Statement, rejected an amendment proposed by the Data Protection Unit that would have maintained a reference to biometric data in the Privacy Statement. As a result, the Privacy Statement contained no reference to biometric data after the amendment. As outlined below, at the time under consideration, members of the Data Protection Unit took the view that it was clear that the Department does process biometric data as part of its SAFE Registration process. On the other hand, an official in the Department's Client Identity Services Unit took the view that the SAFE Registration process does not process biometric data. In his statement to the DPC, the Secretary General explained that his decision to reject the Data Protection Unit's amendment was based on distinguishing between collecting and processing biometric data. It follows from this submission that the Secretary General was not rejecting the Data Protection Unit's position that the Department does process biometric data in making his decision. Therefore, in considering whether the Secretary General gave due weight to the advice rendered by the DPO and the Data Protection Unit (and therefore whether they were properly involved in accordance with Article 38(1)), it is necessary to have regard to the Secretary General's rationale for rejecting the amendment proposed by that Unit.

3.10 The explanation put forward by the Secretary General in his statement submitted to the DPC must be assessed in light of how *collection* is only one form of *processing* of personal data and a controller's obligations in terms of transparency under GDPR relate to the broad range of processing of personal data it conducts. The effect of the Department's amendment was to remove the only reference to biometric data from the Privacy Statement without acknowledging that the Department processes biometric data. On the face of it, this appears in line with the position put forward by the Department's Client Identity Services Unit (that the SAFE Registration does not process biometric data), rather than the position of the Data Protection Unit. In circumstances where the Department has maintained throughout this Inquiry that it has at all times acknowledged that it processes biometric data and that this did not form a basis for rejecting the Data Protection Unit's proposed amendment, it is relevant to question why the Department and the Minister were taking a narrow approach to biometric data at the relevant time under consideration in this Inquiry by explicitly referencing biometric data only in terms of whether they *collected* it or not. While the question of clarity regarding the processing of biometric data is beyond the scope of this

Inquiry and this Decision focuses on Article 38 compliance, it would be remiss not to have regard to this factual background. As outlined below, the Secretary General's rationale for rejecting the proposal of the Data Protection Unit is crucial to determining whether he gave due weight to the advice rendered by the DPO and the Data Protection Unit, and, thus, whether there was an infringement of the requirement of proper involvement in Article 38(1) GDPR. The Draft Decision provisionally accepted the *bona fides* of the explanation put forward by the Secretary General, that is, that the Secretary General was seeking to distinguish collecting biometric data from processing biometric data, and that it was not his intention to deny that the Department processes biometric data. It is highly relevant to this finding to consider how the Secretary General's amendment to the Privacy Statement mirrored the narrow approach taken in the responses to the parliamentary questions and the media query in circumstances where the effect of the amendment was also to deny that the Department *collects* biometric data, without expressly acknowledging, or expressly denying, that the Department processes biometric data. I consider that this consistency in approach is crucial to assessing the explanation put forward in the Secretary General's statement, submitted to the DPC one year after the amendment. The fact that a similar approach was adopted before, and at the time of, the amendment lends credibility to the Secretary General's claim that he was not simply following the interpretation put forward by the Client Identity Services Unit that the SAFE Registration does not process biometric data, but rather gave due weight to the approach put forward by the Data Protection Unit and rejected it based on the Department's pattern of distinguishing between collecting and processing personal data. However, for the avoidance of all doubt, I would emphasise that this Decision does not consider, nor does it make any findings in relation to, the impact that this distinction may or may not have had on the Department's compliance with its transparency obligations. In the context of this Decision, the distinction is relevant to considering the Department's compliance with its obligation in Article 38(1) only, specifically whether the Secretary General gave due weight (in accordance with the requirement of proper involvement) to the advice rendered by the Data Protection Unit. The consistently narrow approach adopted, both before and at the time of the amendment, is directly relevant because it suggests that the Secretary General agreed with the Data Protection Unit that the Department processes biometric data, but rejected their proposed amendment based on the distinction. The Department submitted the text of the responses to the parliamentary questions and the media query during the Inquiry. In circumstances where this information is relevant to assessing whether the Secretary General gave due weight to the Data Protection Unit's advice before rejecting it, and thus whether there was an infringement of the requirement of proper involvement in Article 38(1), I do not accept the Department's submission on the Draft Decision that this information and analysis should be excised from the Decision.

3.11 Returning to the factual background, the Department drafted its Privacy Statement through a structured process that included the Principal Officer who later became the DPO and the Department's Data Programme Management Board. The Board approved the Privacy Statement on 22 May 2018. The approved Privacy Statement included the reference to the collection of biometric data. This reference to biometric data was a new addition to the Privacy Statement in May 2018.

3.12 On 27 June 2018, the Department's DPO provided internal advice on the question of biometric data to members of the Department's Client Identity Services Unit. The DPO advised that the situation concerning the Minister's answers to the Parliamentary Questions *"may now have changed with the coming into effect of the GDPR"*. The DPO suggested that the Department should clarify this with their legal advisors. On the same day, the Department's Client Identity Services Unit confirmed that they had sought legal advice on the issue.

3.13 On 4 July 2018, the Department received a media query in relation to the Privacy Statement's reference to biometric data. The query attached the Department's Privacy Statement and posed the following questions:

> *"I'm wondering if the department has revised its position that it doesn't process biometric data, as stated several times by the Minister. If this is the case, what is the basis for that change?*
>
> *I'm also looking to find out if any or all of the equipment used to take facial images for the purposes of SAFE registration for the PSC captures eye scans/iris scans?"*

3.14 This query set off a series of internal email threads and discussions within the Department on 5 July 2018 questioning the reference to biometric data. The various email threads over the course of the day included a number of officials from the Department. The DPO was on annual leave that day, but replied to emails and had a number of phone calls on the issue throughout the day. The content and precise timings of those emails are set out below.

3.15 At 08:52am, the Department's Press Office forwarded the media query to an official in the Department's Client Identity Services Unit (**"the CIS Official"**) and asked for a draft response. At 09:34am, the CIS Official informed the Department's Press Office that *"in the context of SAFE registration we do not process biometric data and there has been no change in the position."* The CIS Official then set out the following proposed response to the media query:

> *"**Response:***
>
> *With regard to SAFE registration there has been no change in the position. The Department uses Facial image matching software to strengthen the SAFE registration process. In addition, the Public Services Card (PSC) which is the physical token provided from SAFE registration does not store biometrics. While the card does store the person's photograph and it appears on the card, it does not store any biometric or arithmetic template of that photograph.*
>
> *A standard digital photograph in JPEG format is captured during the SAFE registration process and is inputted into and stored in this facial Image matching software. It is then modelled and searched against the Department's photo database to ensure that the person in the photograph has not already been registered using a different*

Personal Public Service Number or a different Identity dataset. It is a similar approach to that taken by the Passport Office in its systems when processing passport applications/renewals.

None of the equipment or processing involved in the SAFE registration process captures eye scans/iris scans nor is there any Intention to do so.

***Ends**"*

The DPO was included on the email at 08:52am and the response at 09:34am. However, other members of the GDPR/DPO Unit were not originally included on that email thread.

3.16 At 08:57am, the DPO forwarded the Press Office's original query to three officials in the GDPR/DPO Unit. At that stage, those officials did not have sight of the CIS Official's reply stating that the SAFE Registration does not process biometric data. Hence, those officials were aware of the media query, but were unaware of the CIS Official's interpretation of the question in relation to biometric data at that stage.

3.17 At 11:30am, one of the officials in the GDPR/DPO Unit (**"the GDPR/DPO Unit Official"**) replied to the DPO. This reply acknowledged that the DPO might not be picking up his emails. The reply proceeded to provide a thorough interpretation of the concept of biometric data in the GDPR. The GDPR/DPO Unit Official concluded as follows:

"The bottom line from a GDPR perspective is that the Department does have the technical means to allow the unique identification of data subjects. In doing so, we are covered by the GDPR definition of biometrics. While recitals are not part of the GDPR themselves, they do demonstrate the rationale behind the relevant articles and allow for certain clear understanding of the Regulation. It seems clear to the DPO that the Department does process biometric data. Therefore the Department's privacy statement, required by Articles 12 of the GDPR includes reference to this processing."

The email only included members of the GDPR/DPO Unit and did not include the Press Office or the CIS Official.

3.18 In interview with the DPC, the DPO confirmed that he had phone calls with the GDPR/DPO Unit Official on 5 July 2018 regarding the Privacy Statement. In those phone calls, the DPO suggested that the GDPR/DPO Unit Official contact the Assistant Secretary for HR and Employment Affairs, who also held responsibility for data protection within the Department and was and was the direct line manager for the DPO. The DPO also stated in interview that the GDPR/DPO Unit Official went to the Department's office on Store Street to discuss the Privacy Statement with the Assistant Secretary for HR and Employment Affairs, the Assistant Secretary for Pensions Policy and North West Centralised Schemes, and a Principal Officer. On this basis, the DPO stated in interview with the DPC that:

"I was entirely satisfied that the views of the DPO were included in the overall consideration of the matter by the Secretary General."

3.19 At 11:51am, the GDPR/DPO Unit Official emailed the Assistant Secretary for HR and Employment Affairs. This email outlined the same analysis in the email at 11:30am, again leading to the conclusion that the Department does process biometric data. At this point, the GDPR/DPO Unit Official had read the CIS Official's response and suggested:

> *"I have read [the CIS Official's] reply to the Irish Times query (see message string below). [The DPO] has suggested that we might be able to get a substantive ruling from the legal advisors as a matter of urgency on this, but this request should possibly come from you? As you can see, we consider the issue to be clear from a GDPR perspective. We had understood that the DMPB had agreed and the Privacy Statement was published on that basis."*

The Press Office and the CIS Official were not included on that email. The DPO was included on the email.

3.20 Meanwhile, at 11:07am, the Press Office emailed the GDPR/DPO Unit Official asking for a response to the media query by that afternoon in circumstances where the DPO was on annual leave. This email also included the CIS Official's earlier response, which is how the GDPR/DPO Unit Official became aware of the CIS Official's response.

3.21 At 15:12pm, the GDPR/DPO Unit Official responded to the Press Office as follows:

> *"We have no objection to [the CIS Official's] response on the matter.*
>
> *For your Information only - the Department's privacy statement, which was uploaded for 25th May is currently under review. The reference to the collection of biometric data is incorrect and will be amended as part of this review. The correct wording of section 3.3 of the privacy statement may therefore be (subject to the ongoing review)-*
>
> *'At times, we also need to ~~collect~~ process 'special categories' of personal data such as data concerning health and biometric data used for the purpose of identification and, at times, information concerning trade union membership.'"*

The CIS Official and the DPO were included on this response. However, the GDPR/DPO Unit Official did not correct the CIS Official's statement in the email at 09:34am that the SAFE registration does not process biometric data. Furthermore, it did not include the GDPR/DPO Unit Official's clear analysis from earlier emails stating that the Department does process biometric data, which the Press Office and CIS Official were not included on. At 15:20pm, the DPO acknowledged the GDPR/DPO Unit Official's response and thanked him for it.

3.22 At 17:42pm the GDPR/DPO Unit Official issued another email advising on the matter. The official sent this email to the Head of Communications and this was the first time that the Head of Communications was included on any of the relevant emails that day. However, it is clear from the email that the GDPR/DPO Unit Official had discussed the issue with the Head of Communications earlier in the day. The GDPR/DPO Unit Official stated:

"As discussed, the GDPR team has no issue with the immediate change of the work "collect" to "process" in section 3.3 of the Department 's privacy statement.

However, also as mentioned, the Statement is currently under review in relation to content & language. We may have other revisions next week.

I note you will also discuss the biometric issue again with [the Assistant Secretary for Pensions Policy and North West Centralised Schemes]."

The Press Office, the CIS Official and the DPO were included on this email.

3.23 In interview with the DPC, the DPO confirmed that he saw this email soon after the GDPR/DPO Unit Official sent it. The DPO emphasised in interview that he was in continuous contact with the GDPR/DPO Unit Official throughout the day. The DPO also stated that he:

"…wouldn't like to give the impression that the decision was made in my absence; I was in contact with the office during the day on a continuous basis".

3.24 In his statement to the DPC included with the Department's submissions on the Draft Inquiry Report, the DPO stated that:

"I was involved in the drafting and the design of the Privacy Statement. Although I was out of the office on annual leave on 5th July, I was involved properly and in a timely manner in consideration on that day as to the situation. I was not involved in the decision as to the final wording of the Privacy Statement which was made by the Secretary General in his role as data controller."[5]

3.25 At approximately 17:45pm, the Head of Communications verbally updated the Secretary General on the matter and informed him of the proposed change suggested by the GDPR/DPO Unit Official (which would simply replace the word *"collect"* with *"process"*). The Secretary General was not included in any of the emails or discussions up to that point. The Secretary General rejected this proposed change. The Secretary General's rationale for rejecting that proposal is set out in his statement to the DPC:

"I considered the change suggested by the DPO team but felt that it did not accurately reflect the Department's approach to the collection of data particularly given the wider context of the press enquiry which had identified the error (see further at 6 and 7 below). I asked the Head of Communications to draft an alternative form of wording

[5] Statement of the Data Protection Officer, dated 22 July 2019.

that would accurately describe the data that the Department actually collected and subsequently approved the text submitted."[6]

3.26 The context in which the Secretary General rejected the proposed change occurred in circumstances where the Department *"distinguishes between the collection, and printing on the PSC, of a simple jpeg image and the subsequent creation and internal use of biometric data from this image as part of a separate data processing process."*[7] The Secretary General outlined to the DPC that there had been media reports in August 2017 incorrectly alleging that the Department used advanced facial scanning cameras to identify people in the Department's offices, that the Public Services Card stored a biometric facial scan, and that the Department shared this scan with other bodies. The Secretary General outlined the Department's distinction between its collection of photographs and processing biometric data. Its position is that the photographs that it collects for the SAFE registration are not biometric data. However, the Department's position is that it uses the photographs to create biometric data in the form of arithmetic templates. This distinction is important to the Department in emphasising to data subjects that it does not use advanced facial image scanning cameras for data collection and real time identity verification purposes. In this regard, the media query received on 4 July asked if any of the equipment used to take facial images for the purposes of SAFE registration captured eye scans/iris scans.

3.27 At 18:07pm, the Head of Communications emailed the Secretary General of the Department with a revised text of paragraph 3.3 of the Privacy Statement (the version quoted at paragraph 3.2 above). The email stated:

"As discussed, there is an error in the GDPR statement on online.

Can you please confirm if the text below is correct?

Once confirmed, we can update the website and tomorrow let the journalist know it was simply a text error."

This email included the DPO, the GDPR/DPO Unit Official, the Head of Communications, the Press Office, the Assistant Secretary for HR and Employment Affairs, and the Assistant Secretary for Pensions Policy and North West Centralised Schemes. The DPO stated in interview with the DPC that he saw this email around the time that it was sent. The email at 18:07pm did not identify that the amendment would remove the only reference to biometric data in the entire Privacy Statement.

3.28 The Secretary General replied at 18:15 approving the revised text and stating the Department should tell the media reporter that the *"privacy statement referred to biometric data in error"*. The Secretary General also asked the DPO:

[6] Statement of the Secretary General, submitted to the DPC in the Department's response to the Draft Inquiry Report, at page 1.
[7] Statement of the Secretary General, submitted to the DPC in the Department's response to the Draft Inquiry Report, at page 2.

"Can you check the rest of the GDPR info and privacy statement to make sure that we don't refer to collection of biometric data. What we do is that we process photographic data to produce a biometric representation for comparison purposes. But we don't collect or share this data.

Was the privacy statement signed-off by CIS?"

The Secretary General did not ask the DPO to ensure that other parts of the Privacy Statement acknowledge that the Department processes, rather than collects, biometric data.

3.29 At 18:44pm, the GDPR/DPO Unit Official emailed the DPO as follows:

"This was not discussed with me! I wouldn't have agreed to this change. As you know the earlier position was agreed with [the Assistant Secretary for Pensions Policy and North West Centralised Schemes] and I subsequently agreed to a one word change in the existing statement.

Are you happy for the blanket removal of reference to biometric data? Not sure I am!!"

This email was sent to the DPO only; neither the Secretary General nor any of the other officials were included on this email.

3.30 The DPC is not aware of any response issued by the DPO to this email. In interview with the DPC, the DPO stated:

"It was established that [the Privacy Statement] was incorrect on the 5 July by the Secretary General in his role as data controller and accounting officer for the Department. I had no problem with his decision because he made the decision based on his interpretation of the facts. He fully respected the independence and role of the DPO and he was aware of aware of my views. He was perfectly entitled as Secretary General to make that decision."

3.31 The DPO also stated in interview that he neither agreed nor disagreed with the GDPR/DPO Unit Official's view and that he:

"*respected the authority of the Secretary General as the data controller and accounting officer to make that decision based on his expertise and experience."*

3.32 At 18:57, the DPO replied to the Secretary General's email confirming that he would check the GDPR information. The DPO did not object to the revised text and did not raise any of the issues that the GDPR/DPO Unit Official highlighted in the emails at 11:30am and 18:44pm. In respect of the revised wording, in interview with the DPC, the DPO stated that he did not see it necessary to express agreement and that *"it was within the prerogative of the Secretary General to make a different decision based on his expertise and experience"*.

3.33 It is important to note that the DPO also stated in interview with the DPC that he did consider that he was appropriately involved in the amendment to the Privacy Statement and that:

> *"There is a recognition within the Department that the DPO has a statutory independent role under the GDPR."*

3.34 This is consistent with the statement provided by the DPO to the DPC in which the DPO stated:

> *"There is no evidence that the opinion of the DPO was not given due weight. The Secretary General wrote several emails where he clearly documented the reasons for not following the DPO's advice. This follows the guidance from the Article 29 Working Party… Despite being on annual leave on the day in question, the DPO, and his team, were centrally involved in the considerations regarding revisions to the Privacy Statement. Despite being on annual leave I was available by telephone and was in contact with the relevant parties during the day. The fact that the data controller, in this instance, the Secretary General reached a different decision based on his analysis of the facts does not negate the involvement of the DPO, and his team, in a proper and timely manner."*[8]

3.35 Furthermore, in relation to the question of whether the DPO received any instructions, the DPO stated in the statement that:

> *"As DPO at that time, I can clearly and categorically confirm that I did not receive any instructions from the Secretary General, or any Assistant Secretary, in this matter."*[9]

3.36 At 23:48 pm, the Head of Communications emailed the media reporter stating, *"The existing privacy statement referred to biometric data in error."* The remainder of the email consisted of the proposed response provided by the CIS Official that day at 9:34am.

3.37 On the morning of 6 July 2018, the Department updated the revised Privacy Statement on its website. After that revision, the Privacy Statement made no reference to biometric data. Later that day, the Press Office received another query from the media reporter inquiring as to whether the DPO was notified about the changes and whether the DPO authorised them. In response to this query, the Head of Communications suggested that the Department could confirm that the DPO was notified and that he did authorise them.

3.38 The DPO suggested the following alternative response:

> *"In line with the GDPR, the DPO is involved in all issues which relate to the protection of personal data"*

[8] Statement of the Data Protection Officer, dated 22 July 2019.
[9] Ibid.

3.39 The Secretary General replied to this suggestion with an amended response as follows:

> *"In line with the GDPR, the DPO is involved in all issues which relate to the protection of personal data including the correction made in this instance"*

3.40 The DPO responded to the Secretary General's email stating that he was on annual leave and that he *"was not across this correction"*. The Secretary General replied stating that he understood that the DPO, or his staff, had contributed to the reply.

3.41 On 11 October 2018, the DPC received a complaint from Digital Rights Ireland CLG, an organisation mandated under Article 80 of the GDPR to lodge the complaint on behalf of an individual. The complaint alleged a *"serious interference with the independence of the Data Protection Officer (DPO) in the Department of Employment Affairs and Social Protection"* in violation of Article 38 of the GDPR. The complaint also enclosed emails released by the Department under the Freedom of Information Act 2014. The DPC explained to Digital Rights Ireland that it could not treat the complaint as an individual's complaint for the purposes of Article 77 GDPR as there was no assertion of processing of her personal data contained in the complaint but that it would in any case examine the issues raised in its submission.

3.42 The Inquiry Team informed the Department of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry on 5 December 2018. The Notice set out the scope and legal basis of the Inquiry. The decision to commence the own volition (rather than complaint-based) inquiry was taken having regard to the complaint and the documents provided by the Department to the complainant under the Freedom of Information Act 2014. The Inquiry Team was of the view that an inquiry was necessary in order to ascertain whether one or more provisions of the GDPR may have been contravened. The Notice set out that the Inquiry would establish a full set of facts so that it might assess whether or not the Department had discharged its obligations as data controller and/or data processor in connection with the subject matter of the allegations and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the Department in that context. In this regard the Notice set out that the Inquiry would focus on data protection governance and the role of the DPO within the Department in respect of Article 38 of the GDPR. The Notice also set out seven queries that required the Department to produce certain information and documents to the DPC.

3.43 The Department responded to the Notice on 19 December 2018. The Department sought clarifications on the specific provisions and precise allegations subject to the Inquiry. The Department also sought a copy of the complaint made to the DPC. The Department made submissions on its Data Protection Governance and appended its *"Corporate Governance Framework 2018"*, its *"Statement of Strategy 2017-2020"*, and other relevant documents. The Department also provided a response to the seven queries posed by the DPC. On 21 December 2018, the Department wrote to the Inquiry Team providing copies of two emails that it omitted in error from the submissions dated 19 December 2018.

3.44 On 18 January 2019, the Inquiry Team wrote to the Department clarifying that the Articles the subject of the inquiry are Articles 38(1) and (3) of the GDPR and that the purpose of the inquiry is to establish the facts around the allegations that the Department may have interfered with the independence of its DPO. The Inquiry Team confirmed that the correspondence taken into account in relation to the DPC's decision to undertake an own volition inquiry comprised a set of documents released by the Department in respect of the Freedom of Information request. The Inquiry Team detailed those documents in an appendix to the letter. The Inquiry Team also sought copies of further emails and unredacted versions of the emails that the Department had provided to the complainant pursuant to the Freedom of Information Act 2014. The Inquiry Team set out a chronology of events relevant to the Inquiry, based on the interim response of the Department and the information received from the complaint, to allow the Department to make submissions on the chronology and to identify any factual representation with which the Department disagreed.

3.45 On 25 January 2019, the Department responded to the Inquiry Team's correspondence and provided the documentation sought. The Department also made submissions on the chronology of events and made submissions on Article 38(1) and (3) of the GDPR.

3.46 On 15 March 2019, the Inquiry Team wrote to the DPO. The Inquiry Team notified the DPO that it wished to conduct an interview with the DPO in order to further the Inquiry. On 19 March 2019, the DPO confirmed that he was available to attend and sought certain information in advance of the interview. The Inquiry Team wrote to the DPO on 26 March 2019 and provided the information sought, emphasising that the interview would be a voluntary interview and that there was no obligation on the DPO to participate. On 5 April 2019, the DPO attended the DPC's office, Fitzwilliam Square, Dublin 2 for the purpose of the interview. The Inquiry Team presented their official identification, explained the purpose of the interview, and gave a background to the Inquiry. The Inquiry Team also reminded the DPO that there was no legal requirement to respond to the questions; that any responses were to be considered a voluntary statement pursuant to Article 31 of GDPR. The DPO confirmed that he understood and answered all of the questions. On 12 April 2019, the Inquiry Team provided the DPO with a copy of the draft transcript of interview and provided the DPO with an opportunity to make submissions as to its accuracy. On 25 April 2019, the DPO submitted a number of amendments to the draft transcript. The Inquiry Team reviewed the amendments and accepted each of them into the transcript in the circumstances. I have had regard to the transcript of interview for the purposes of this Decision.

3.47 On 28 May 2019, the Inquiry Team provided the Department with a copy of the Draft Inquiry Report and invited submissions by 12 June 2019. On 5 June 2019, the Department sought an extension of the deadline for submissions to 24 July 2019 and specified reasons to justify the extension. The Inquiry Team agreed to the extensions. On 24 July 2019, the Department made submissions on the Draft Inquiry Report. Those submissions included submissions on the provisional views of the Inquiry Team expressed in the Inquiry Report and also included a statement from the Secretary General of the Department and a statement from the DPO at the time. I have had due regard to those submissions and statements for the purposes of this Decision.

3.48 On 8 March 2021, I provided the Department with the Draft Decision and invited submissions by 29 March 2021. The Department made submissions on 29 March and I have had due regard to those submissions in making this Decision.

4. Scope of the Inquiry

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine the sequence of events described in the complaint to the DPC to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by the Department in that context. In this regard, the Notice of the Commencement of the Inquiry stated that the scope would focus on data protection governance and the role of the DPO in respect of the Department's compliance with the obligations under Article 38 of the GDPR. On 19 December 2018, the Department sought clarification on the specific provisions of the 2018 Act/ Article 38 GDPR subject to the Inquiry. By letter dated 18 January 2019, the DPC clarified that the Articles in question were Articles 38(1) and (3) of the GDPR.

5. Issues for Determination

5.1 Having reviewed the Inquiry Report and the other materials provided to me, I consider that the issues in respect of which I must make a decision are:

(i) Whether the Department complied with its obligation pursuant to Article 38(1) of the GDPR to ensure that the DPO was involved, properly and in a timely manner, in the Department's amendment to its Privacy Statement as implemented on 6 July 2018, and

(ii) Whether the Department complied with its obligation pursuant to Article 38(3) of the GDPR to ensure that the DPO did not receive any instructions regarding the exercise of the tasks referred to in Article 39 of the GDPR in respect of the Department's amendment to its Privacy Statement as implemented on 6 July 2018.

6. Issue 1: Article 38(1)

6.1 Article 38(1) of the GDPR provides:

> *"The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."*

6.2 The obligation in Article 38(1) applies to controllers and processors with a designated DPO and applies in respect of all issues which relate to the protection of personal data. Therefore,

it is first necessary to determine whether the Department was obliged to involve the DPO in the process to amend the Privacy Statement in the circumstances.

i. Whether the Department was obliged to involve the DPO pursuant to Article 38(1) in the circumstances

6.3 The obligation in Article 38(1) to involve the DPO applies to controllers and processors with a designated DPO. In both its original and revised Privacy Statement, the Department stated that it is *"the Data Controller for all personal data collected for the purpose of its business"*. Regarding its use of photographs, the Department submitted that it *"uses facial image matching software to strengthen the SAFE registration process by detecting and deterring duplicate SAFE registration attempts."*[10] In those circumstances, it is clear that the Department determines the purposes and means of the processing of the digital photographs used in its SAFE Registration process. Therefore, it is the controller in respect of this processing of personal data. As outlined above, at the time under consideration in this Inquiry, the Department had designated a DPO[11].

6.4 The obligation in Article 38(1) to involve the DPO applies to all issues that relate to the protection of personal data. I am satisfied that the Department's amendment to its Privacy Statement was an issue that related to the protection of personal data within the meaning of Article 38(1). Transparency is a fundamental element of the data protection principles set out in Article 5 of the GDPR, and further elaborated on in Articles 12 - 14 of the GDPR. Transparency further facilitates data subjects in exercising their rights under the GDPR. The Article 29 Working Party guidelines on transparency highlight the importance of a controller's Privacy Statement as a modality for transparency and provide that, in addition to layered privacy statements where applicable, *"the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document"*[12]. Amendments to the Department's Privacy Statement not only have the potential to affect the Department's compliance with its transparency obligations, but can also affect data subjects' ability to exercise other rights under the GDPR. Therefore, I am satisfied that the Department's decision to amend its Privacy Statement was an issue that related to the protection of personal data within the meaning of Article 38(1). Furthermore, in circumstances where the Department's Privacy Statement stated that *"This document is being provided to you in line with our obligations under the General Data Protection*

[10] The Department's submissions on the Draft Inquiry Report, dated 24 July 2019, at page 14.
[11] The Department was obliged to do so pursuant to Article 37(1)(a) of the GDPR.
[12] Article 29 Working Party "Guidelines on transparency under Regulation 2016/679", adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, at page 11.

Regulation"[13], I am satisfied that the obligation in Article 38(1) of the GDPR is applicable to all relevant decisions to amend that document[14].

6.5 The Department was obliged to involve the DPO in the process that lead to the amendment to the Privacy Statement on 6 July 2018. The Department is the controller in respect of the photographs that it captures during the SAFE registration process and its Privacy Statement is an important modality for meeting its transparency obligations in respect of its processing of personal data. In the circumstances, the amendments to that statement, regardless of whether they are correct or not, had the potential to affect the transparency of the Department's processing and to affect data subjects' rights. Therefore, as controller, the Department was obliged to ensure that the DPO was involved, properly and in a timely manner, in this issue.

ii. The requirement that the DPO is involved "properly and in a timely manner"

6.6 The standard in Article 38(1) requires that the DPO must be properly involved. The GDPR does not expressly define what constitutes proper involvement. In those circumstances, it is a well-established principle that one must have regard to the context, objective and purpose of the measure when interpreting European Union law. In *Merck v. Hauptzollamt Hamburg-Jonas* the European Court of Justice held:

> *"However, as the Court has emphasized in previous decisions, in interpreting a provision of Community law it is necessary to consider not only its wording but also the context in which it occurs and the objects of the rules of which it is part."*[15]

6.7 In interpreting the requirement of proper involvement, it is appropriate to have regard to the context and objectives of Article 38(1) in light of the GDPR as a whole. This interpretation must secure the effectiveness of Article 38(1) in light of its objectives. For the reasons set out below, it is clear that proper involvement goes beyond requiring that the DPO is informed of issues relating to the protection of personal data. Proper involvement requires a consultative role in which the DPO must have an opportunity to make a meaningful contribution on the issue in question, and in which the controller or processor must give due weight to any advice rendered.

6.8 Proper involvement requires that the DPO must have an opportunity to make a meaningful contribution on issues that relate to the protection of personal data. The GDPR provides that

[13] At page 3.
[14] In circumstances where the Privacy Statement did not claim to be provided to data subjects in line with any obligations that the Department may or may not have been under pursuant to Part 5 of the Data Protection Act 2018 or Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 ("The Law Enforcement Directive"), I do not consider it necessary, for the purposes of this decision, to consider whether the particular processing operations concerning the photographs captured during the SAFE Registration process falls under those provisions, or the GDPR, or both.
[15] Merck v. Hauptzollamt Hamburg-Jonas, Case 292/82, [1983] E.C.R. 1-3781, 3792, at paragraph 12.

DPOs should be designated based on their professional qualities, including expert knowledge of data protection law[16]. The purpose of Article 38(1) is to ensure that this expertise is available on all issues that relate to the protection of personal data. The Article 29 Working Party Guidelines on Data Protection Officers outline how ensuring that the DPO is informed and consulted facilitates compliance with the GDPR and promotes a privacy by design approach[17]. I consider that the purpose of Article 38(1) would be defeated if the requirement of proper involvement could be satisfied by simply informing the DPO of issues relating to the protection of personal data. Proper involvement requires that the DPO must have an opportunity to make a meaningful contribution on those issues in the circumstances.

6.9 The opportunity to make a meaningful contribution does not bestow a decision-making role on the DPO beyond their tasks pursuant to Article 39. To the contrary, the controller, as the entity accountable for complying with the GDPR, is ultimately responsible for making decisions on measures implemented to ensure, and to be able to demonstrate, compliance with the GDPR. Therefore, controllers may accept or reject any advice rendered by the DPO pursuant to Article 38(1).

6.10 Proper involvement does require that the controller or processor must give due weight to any advice rendered by the DPO, despite the fact that the controller or processor is not obliged to follow that advice. The Article 29 Working Party Guidelines on Data Protection Officers provide that:

> *"The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice."*[18]

This is consistent with the purpose of Article 38(1). In order for a DPO to be properly involved, the decision-maker on a data protection issue must give due weight to any advice provided by the DPO. This reflects the expert advisory role envisaged by the GDPR. A DPO is not properly involved if the controller discards their advice without proper consideration or if the decision maker for the controller does not have access to, or does not consider, the DPO's advice.

6.11 It is important to note that Article 38(1) does not regulate the content or form of any advice that a DPO may provide, nor does it require that a DPO must actually decide to provide advice on any issue. The content and form of any advice rendered by a DPO, including the question

[16] Article 37(5) GDPR.

[17] Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')", Adopted on 13 December 2016, as last revised and adopted on 5 April 2017, at page 13 provides:
"Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation."

[18] Ibid at page 14.

as to whether to provide advice on a particular issue, are properly matters for the DPO's own expert judgement.

6.12 Article 38(1) is silent on the extent to which the involvement of data protection professionals working under the supervision of the DPO can fulfil the requirements of the Article. The Article 29 Working Party Guidelines on Data Protection Officers acknowledge that it may be necessary to set up a DPO team in some organisations[19]. Article 39 GDPR sets out a diverse and non-exhaustive variety of tasks for the DPO as a minimum. The obligation in Article 38(1) is broad and applies to *"all issues"* relating to the protection of personal data. In some organisations, it may be necessary for the DPO to have support from a team in order to perform the DPO's tasks efficiently. This support will facilitate, rather than hinder, compliance with the GDPR by ensuring that the DPO has adequate resources to perform their tasks effectively. In some instances, the GDPR requires prompt action from a controller on issues that relate to the protection of personal data[20]. Delivering action without undue delay may require a significant contribution from members of a data protection team in some instances. Therefore, for the purposes of Article 38(1), I am satisfied that it is appropriate to have regard to the involvement of data protection team members if they are working under the direct supervision of the DPO in respect of the issue.

6.13 The obligation to involve the DPO in a timely manner requires that the DPO must be involved at a point in time in which the organisation is deciding its course of action in respect of the data protection issue. It is not sufficient for the DPO to be involved after the organisation has made its decision, in a binary approval/disapproval role. The DPO must be involved at the creative stage of formulating a response, and not just in implementing that response. The obligation to involve the DPO in a timely manner under Article 38(1) must be read in light of the objective of achieving compliance with the GDPR generally. When the DPO's expertise is available as soon as practicable after the controller identifies a data protection issue, this promotes compliance with data protection by design pursuant to Article 25 GDPR. For this reason, the Article 29 Working Party guidelines on Data Protection Officers provide that *"It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection"*[21]. Even where a data protection issue arises after the design stage of a project, this early involvement of the DPO in creating the organisation's course of action is crucial to ensure that the organisation effectively implements data protection in all its processing operations. The obligation to involve the DPO in a timely manner also requires that all relevant information necessary for the DPO to advise on that data protection issue

[19] Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')", Adopted on 13 December 2016, as last revised and adopted on 5 April 2017, provides at page 14:
"Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up."

[20] For example, a controller's obligation to notify certain personal data breaches to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it pursuant to Article 33(1) of the GDPR.

[21] Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')", Adopted on 13 December 2016, as last revised and adopted on 5 April 2017, at page 13.

must be provided at a point in the timeline that enables the DPO to make a meaningful contribution.

iii. Whether the Department complied with its obligation to ensure that the DPO was involved properly and in a timely manner

6.14 In determining whether the DPO was properly involved in the amendment to the Privacy Statement, I must first consider whether the DPO had an opportunity to make a meaningful contribution on the issue. I must then consider whether the Department gave due weight to any advice actually rendered.

6.15 It is clear that the Department did not simply inform the DPO of the media query in a trivial way, but rather consulted the DPO and his team with the purpose of inviting a meaningful contribution in developing the Department's course of action. The Department informed the DPO of the original media query soon after receiving it. Furthermore, the DPO was the only official included on all of the pertinent emails on 5 July 2018 as set out in Part 3 of this Decision. However, the DPO was on annual leave and this is relevant to assessing whether he had an opportunity to make a meaningful contribution in the circumstances. In light of this fact, it is necessary to consider any direct contribution made by the DPO on 5 July 2018, any contact he had with his team, and the involvement of those team members if working under his direct supervision.

6.16 It is significant that the DPO was on annual leave on 5 July 2018. However, this fact alone does not provide a full picture of the DPO's involvement throughout the day. The DPO sent three emails on the issue over the course of the day (at 08:57am, 15:20pm and 18:44pm). He was also in continuous contact with the GDPR/DPO Unit Official. At no point did he suggest that the Department should postpone the question of amending the Privacy Statement until his return from annual leave the following day.

6.17 In his interview with the DPC and in his statement submitted to the DPC, the DPO consistently maintained that he was involved in the consideration of the issue throughout the day. This position is also consistent with the emails sent throughout the day. In both the interview and the statement, the DPO stated his view that he was involved in a proper and timely manner in the amendment to the Privacy Statement.

6.18 As outlined above, in considering whether there was an infringement of Article 38(1), I must have regard to any involvement of DPO team members if they are working under the direct supervision of the DPO. On the facts, it is clear that the GDPR/DPO Unit Official was working under the direct supervision of the DPO at the relevant time. After forwarding the original press query to his team, the DPO maintained contact with the GDPR/DPO Unit Official throughout the day and had phone calls with that official. He suggested by email that the GDPR/DPO Unit Official contact the Assistant Secretary for HR and Employment Affairs. The DPO sent an email at 15:20pm to acknowledge the advice provided by the GDPR/DPO Unit Official to the Press Office. The facts establish that the DPO maintained contact with his team

throughout the day and supervised the advice provided by the GDPR/DPO Unit Official in respect of the amendment to the Privacy Statement.

6.19 In the circumstances, I find that the DPO did have an opportunity to make a meaningful contribution to the amendment to the Privacy Statement. I have had particular regard to the level of direct involvement that the DPO had on 5 July 2018, how he maintained contact with his team throughout the day, and the involvement of the GDPR/DPO Unit Official working under the DPO's supervision. Not only did the DPO have the opportunity to make a meaningful contribution, but also the GDPR/DPO Unit Official subsequently exercised that opportunity under the DPO's supervision. When the Press Office asked the DPO's team directly for a response to the press query, the DPO was included on that email. The GDPR/DPO Unit Official, following phone calls with the DPO, then contributed to the issue of amending the Privacy Statement by providing advice in the emails at 15:12pm and 17:54pm and in the discussions in Store Street. Therefore, I am satisfied that the DPO not only had an opportunity to make a meaningful contribution to the amendment to the Privacy Statement, but also exercised that opportunity through his team.

6.20 The Secretary General did not follow the approach advised by the GDPR/DPO Unit Official. The Secretary General was entitled to do this because Article 38(1) does not oblige controllers to follow any advice rendered. The DPO and his team were included on the Head of Communication's email at 18:07pm to the Secretary General with the new proposed amendment. The facts establish that the DPO actively decided not to contribute to the issue any further at this point. This is despite the fact that the GDPR/DPO Unit Official emailed the DPO at 18:44pm identifying that the proposed amendment would result in a blanket removal of the reference to biometric data and stating that he was not happy with that. Notwithstanding that advice, the DPO decided not to bring it to the Secretary General's attention and replied to the Secretary General at 18:57pm confirming that we would check the GDPR information generally for any other reference to the collection of biometric data. The DPO confirmed this in interview with the DPC when he stated that he *"neither agreed nor disagreed with [the GDPR/DPO Unit Official]"*. I am satisfied that the DPO's decision not to advise further was based on this uncertainty, and that it was not based on any lack of opportunity to make a meaningful contribution in the circumstances. The DPO's position in interview is consistent with the email on 27 June 2018 in which he advised that the Department should seek legal advice on the matter.

6.21 Article 38(1) does not regulate the content or form of any advice that a DPO may provide, nor does it require that a DPO must actually decide to provide advice on any issue. The DPO's decision not to advise further on the revised amendment cannot give rise to an infringement of Article 38(1). That Article must leave discretion with DPOs to decide on the form and content of any advice that they may give, and to decide on the question of whether to provide advice in the first place. In the circumstances, it is not the case that the DPO and his team were excluded from the Secretary General's decision to make the changes to the Privacy Statement. It is clear that the DPO and his team had the opportunity to make a meaningful contribution to the amendment to the Privacy Statement. They exercised that opportunity by advising on the issue and, as outlined below, the Secretary General had regard to that

advice. They had a further opportunity to make a meaningful contribution after the Secretary General rejected the advised approach and before the Privacy Statement was amended the next morning, but the DPO actively decided not to contribute further. Therefore, in all the circumstances, the Department did provide the DPO with an opportunity to make a meaningful contribution to the amendment to the Privacy Statement.

6.22 In determining whether the Department gave due weight to the advice rendered by the DPO and his team, I must focus on the role of the Secretary General as decision maker in relation to the amendment to the Privacy Statement. The Secretary General was not included on the emails or discussions in which the GDPR/DPO Unit Official rendered his advice. Instead, the Press Office and the Head of Communications drove the process to amend the Privacy Statement by dealing with the original press query, seeking the advice of the GDPR/DPO Unit Official, briefing the Secretary General, and drafting the alternative amendment to the Privacy Statement. In light of how the Department conducted this process, I must consider whether the Secretary General was aware of the GDPR/DPO Unit Official's advice. The onus was on the Department to ensure that the decision maker was aware of, and gave due weight to, any advice rendered by the GDPR/DPO Unit Official. In the circumstances, a failure on the part of the Press Office or the Head of Communications to communicate such advice rendered would infringe Article 38(1).

6.23 The GDPR/DPO Unit Official's position is clear when considered in light of all of the relevant emails sent on 5 July 2018. That official's view was that the Department could justifiably amend paragraph 3.3 of the Privacy Statement so that it stated that the Department *processes* rather than *collects* personal data. The emails internal to GDPR/DPO Unit further illustrate that the official's position was that the Privacy Statement must reference the fact that the Department processed biometric data. However, the GDPR/DPO Unit Official communicated this advice to other members of the GDPR/DPO Unit only and did not include this advice in the emails to the Press Office, the Head of Communications, or the Secretary General.

6.24 As outlined above, the content and form of any advice rendered by a DPO, including the question as to whether to provide advice on a particular issue, are properly matters for the DPO's own expert judgement. In considering whether the Secretary General gave due weight to the advice rendered, I can only have regard to advice actually rendered and I cannot have regard to internal discussions within the GDPR/DPO Unit. The GDPR/DPO Unit Official's first email advising on the issue was at 15:12pm. This email stated that the Unit has *"no objection to [the CIS Official's] response on the matter"*, but did not address the CIS Official's statement that the SAFE Registration does not process biometric data. The email went on to state that the *"reference to the collection of biometric data is incorrect"* and suggested a correct wording that replaces the word *"collect"* with *"process"*. The email does not refer to that official's own earlier analysis on how the Privacy Statement must reference the fact that the Department processes biometric data.

6.25 The GDPR/DPO Unit Official followed up on that first email with further advice in a second email at 17:42pm. In this email, the official stated that *"the GDPR team has no issue with the*

immediate change of the work 'collect' to 'process' in Section 3.3 of the Department's privacy statement". The official also stated in that email *"I note you will also discuss the biometric issue again"* with another official. This email does not refer to the earlier analysis on how the Privacy Statement must reference the fact that the Department processes biometric data.

6.26 Before sending those emails, the GDPR/DPO Unit Official went to the Department's office on Store Street and had discussions with officials on the Privacy Statement. The subsequent emails at 17:42pm and 18:44pm gives insight to the content of those discussions. In the email at 17:42am, the GDPR/DPO Unit Official noted that the word *collect* could be replaced with the word *process*, that there may be other revisions the following week, and that the Head of Communications would discuss the biometric issue again with another official. It is clear that the GDPR/DPO Unit Official understood at that point that the amendment to the Privacy Statement would focus on the *collect v process* distinction and that it would still reference the Department's processing of biometric data. In the email at 18:44pm to the DPO, in which the GDPR/DPO Unit Official expressed disagreement to the blanket removal of the reference to the processing of biometric data, the GDPR/DPO Unit Official stated that the broader amendment *"was not discussed with me! I wouldn't have agreed to this change"*. Therefore, the discussions in Store Street likely did not specifically address the blanket removal of the reference to biometric data.

6.27 However, the email at 18:44pm, like the email at 11:30am, was internal to the GDPR/DPO Unit. The DPO actively decided not to advise on the blanket removal of the reference to biometric data in his response to the Secretary General. Both the DPO and the GDPR/DPO Unit Official had the opportunity to advise on this, but didn't do so. Therefore, in determining whether the Department gave due weight to the advice rendered by the DPO and his team, I cannot have regard to the earlier thorough interpretation of the concept of biometric data provided by the GDPR/DPO Unit Official in internal emails within the GDPR/DPO Unit.

6.28 I am satisfied that the Secretary General did give due weight to the advice actually rendered by the DPO and the GDPR/DPO Unit Official. The Secretary General outlined in his statement provided to the DPC that he considered the change suggested by the DPO team but rejected it because he *"felt that it did not accurately reflect the Department's approach to the collection of data"*. The explanation outlined in the Secretary General's statement mirrors the approach taken by the Minister in response to the parliamentary questions and the Department's response to the media query, both before and at the time of the amendment respectively. It is also consistent with how Part 3 of the Privacy Statement was titled "*"What types of Personal Data do we Collect"*. The Secretary General's focus was on the Department's distinction between collecting biometric data and processing biometric data. While this resulted in a blanket removal of the only reference to biometric data in the Privacy Statement, the DPO and his team's analysis of this issue was internal to that team only. Furthermore, as detailed earlier in this Decision, the question of whether the amendment ultimately impacted on the Department's compliance with its transparency obligations is outside the scope of this Inquiry. The Secretary General, in his statement to the DPC, outlined that he asked the DPO to check the GDPR material for other references to the collection of biometric data because the DPO was most familiar with these documents. This suggests that

the Secretary General may not have been aware that the amendment would result in a blanket removal of any reference to biometric data in the Privacy Statement. This is consistent with how the advice on that particular issue was not communicated outside of the GDPR/DPO Unit. Notwithstanding, it is clear that certain advice actually rendered by the DPO and the GDPR/DPO Unit Official was communicated to the Secretary General and that the Secretary General gave due weight to that advice. This includes the Data Protection Unit's proposed amendment that would have maintained a reference to biometric data in the Privacy Statement. I am satisfied that the Secretary General's rationale for rejecting this proposal was based on the Department's distinction between collecting and processing personal data and does not reflect a failure to give due weight to the advice rendered by the DPO and the Data Protection Unit. On the established facts, I do not consider that the Secretary General was adopting the position put forward by the CIS Official that the SAFE Registration does not process biometric data. While the Secretary General's approach resulted in the Department removing the only reference to biometric data from the Privacy Statement, it is not within the scope of this Decision to consider whether the Department complied with its transparency obligations in that regard. I am satisfied that the Secretary General did give due weight to the advice actually rendered by the DPO and the GDPR/DPO Unit Official.

6.29 In determining whether the DPO was involved in a timely manner, it is necessary to consider whether the DPO was involved at a point in time in which the Department was deciding its course of action in respect of the Privacy Statement. It is also necessary to consider whether the DPO had access to all relevant information at a point in the timeline that enabled the DPO to make a meaningful contribution. In the circumstances, it is clear that the DPO was involved in a timely manner. The Department received the press query on the evening of 4 July 2018 and the Press Office included the DPO on their first request for a draft response the following morning. As outlined above, the DPO was also included on all pertinent emails throughout the day, including when the Department formulated its first response, and the later revised amendment. It is also clear that the DPO had access to all relevant information from the Press Office's first email, which attached the press query. The DPO had previously advised the Department's Client Identity Services Unit on the issue of biometric data on 27 June 2018. This shows that the DPO had previously considered the issue and had access to the necessary information in order to advise on the issue. Further, the DPO at no point requested that consideration of the issue be deferred pending his return from one day's annual leave. To the contrary, the DPO's interview with the DPC establishes that he was substantially involved in the amendment to the Privacy Statement throughout the day.

iv. Finding

6.30 I find that the Department involved their DPO, properly and in a timely manner, in the Department's amendment to its Privacy Statement as implemented on 6 July 2018. Therefore, the Department did not infringe Article 38(1) of the GDPR in the circumstances.

7. Issue 2: Article 38(3)

7.1 Article 38(2) & (3) of the GDPR provide as follows:

> *"2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.*
>
> *3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."*

7.2 The obligation in Article 38(3) to ensure that the DPO does not receive any instructions regarding the exercise of *"those tasks"* structurally relies on the preceding sub-article. Article 38(2) makes clear that the tasks referred to in Article 38(3) are the *"tasks referred to in Article 39"*.

7.3 Article 39(1) of the GDPR provides:

> *"The data protection officer shall have at least the following tasks:*
>
> *(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*
>
> *(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*
>
> *(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;*
>
> *(d) to cooperate with the supervisory authority;*
>
> *(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."*

7.4 Article 38(3) provides autonomy to DPOs by ensuring that they do not receive instruction regarding the tasks referred to in Article 39. This ensures the independence of the DPO when carrying out those tasks. However, it is not the purpose of Article 38(3) to prohibit all possible instructions that may be given to a DPO as part of an ordinary employment relationship.

7.5 The tasks in Article 39(1)(a) include advising the controller or processor on their obligations under the GDPR. As outlined above, where a controller or processor disagrees with advice rendered by the DPO, they may decide not to follow it. In such circumstances, the Article 29 Working Party recommends, as good practice, to document the reasons for not following the DPO's advice[22]. Article 38(3) clearly prohibits a controller from instructing the DPO to interpret the law in a particular manner or to arrive at a particular conclusion in their advice. This includes circumstances where a controller may seek to avoid documenting their disagreement with the advice of the DPO. However, where a controller disagrees with the DPO's independent and autonomous advice, the GDPR does not prevent that controller from providing instructions to the DPO in relation to implementing the controller's preferred approach once those instructions do not relate to the Article 39 tasks. On the contrary, as such matters will relate to the protection of personal data, it is entirely proper for the DPO to be involved in implementing the controller's decision.

7.6 The Secretary General's email at 18:15pm on 5 July 2018 asked the DPO to *"check the rest of the GDPR info and privacy statement to make sure that we don't refer to collection of biometric data."* I find that this instruction did not concern the DPO's task of advising the Department of its obligations under data protection law. The Secretary General made this instruction having considered the advice rendered earlier in the day. The instruction did not preclude the DPO from providing further advice and it did not instruct the DPO as to how he should advise the Department in the future. Furthermore, the DPO's statement submitted to the DPC categorically states that he did not receive any instructions regarding the exercise of his tasks.

7.7 The instruction did not relate to how the DPO interpreted the law or the conclusion arrived at. The instruction related to the content of the Privacy Statement and I accept that the Secretary General's focus was on the Department's distinction between collecting biometric data and processing biometric data. As outlined above, the Department, as the entity accountable for complying with the GDPR, is ultimately responsible for making decisions on measures implemented to ensure, and to be able to demonstrate, compliance with the GDPR. Therefore, the Secretary General is entitled to make decisions regarding the content of the Privacy Statement. It is outside the scope of this Inquiry to determine whether the Department complied with its transparency obligations. However, it is clear that the Secretary General did not provide any instruction to the DPO regarding his task under Article 39(1)(a) of advising the Department. It is also clear that the Secretary General's instruction did not relate to the exercise of any of the other tasks referred to in Article 39.

[22] Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')", Adopted on 13 December 2016, as last revised and adopted on 5 April 2017, at page 14.

i. Finding

7.8 I find that the Department did not provide any instructions to the DPO regarding the exercise of the tasks referred to in Article 39 of the GDPR in respect of the Department's amendment to its Privacy Statement as implemented on 6 July 2018. Therefore, the Department did not infringe Article 38(3) of the GDPR in the circumstances.

8. Right of Appeal

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

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

The Inquiry Team delivered the Final Inquiry Report to me on 11 February 2021. I was also provided with, and have had regard to, all of the correspondence, submissions, and documentation gathered during the Inquiry, including:

(i) The DPC's Final Inquiry Report, Inquiry Reference IN-18-12-01;

(ii) DPC Notice of Commencement of an Inquiry, dated 5 December 2018;

(iii) The Department's cover letter regarding its response to the Notice of Commencement of an Inquiry, dated 19 December 2018;

(iv) Document titled *"Interim Response to the Data Protection Commission's Inquiry Ref: IN 18-12-000001"*, including Part 1 *"Issues and Clarifications"*, Part 2 *"Data Protection Governance"*, and Part 3 *"Responses to DPC's 7 Queries"*, dated 19 December 2018;

(v) The Department's *"Corporate Governance Framework 2018"*;

(vi) The Department's *"Statement of Strategy 2017 - 2020"*;

(vii) A spreadsheet submitted by the Department outlining its identified general corporate risks which refer to Information security/data protection and mitigation measures (Appendix 3 to Part 2 of its interim response to the Notice of Commencement of an Inquiry);

(viii) A spreadsheet submitted by the Department outlining sample BISU and GDPR units activities and risks and (Appendix 4 to Part 2 of its interim response to the Notice of Commencement of an Inquiry);

(ix) A spreadsheet submitted by the Department providing a sample of activities across other business areas which refer to Information security/ data protection (Appendix 5 to Part 2 of its interim response to the Notice of Commencement of an Inquiry);

(x) The Department's Privacy Statement dated May 2018 (as submitted in Part 3 of the Department's *"Interim Response to the Data Protection Commission's Inquiry Ref: IN 18-12-000001"*;

(xi) The Department's amended Privacy Statement (as submitted in response to Query 6 in *"the Department's "Interim Response to the Data Protection Commission's Inquiry Ref: IN 18-12-000001"*;

(xii) Correspondence from the Department to the Inquiry Team, dated 21 December 2018, enclosing 2 emails that were omitted in error from the Department's *"Interim Response to the Data Protection Commission's Inquiry Ref: IN 18-12-000001"*;

(xiii) Correspondence from the Inquiry Team to the Department, dated 18 January 2019, clarifying points raised by the Department and requesting further documentation from the Department;

(xiv) Correspondence from the Department to the Inquiry Team, dated 25 January 2019, appending certain unredacted emails, and making submissions;

(xv) Collated Internal Department Emails between 4 – 6 July 2018, titled DPC 01 – DPC 33 (appendix 6 to the DPC's Final Inquiry Report);

(xvi) Correspondence from the Inquiry Team to the DPO, dated 12 April 2019, enclosing the draft transcript of interview;

(xvii) Correspondence from the DPO to the Inquiry Team, dated 25 April 2019, submitting proposed amendments to the draft transcript of interview;

(xviii) The DPC's transcript of interview with the Department's DPO incorporating the amendments submitted by the DPO on 25 April 2019;

(xix) The DPC's Draft Inquiry Report, dated 10 May 2019;

(xx) Correspondence from the Inquiry Team to the Department, dated 28 May 2019, enclosing the Draft Inquiry Report;

(xxi) Correspondence from the Department, dated 3 August 2018, granting Freedom of Information Request 2018-11019, and the schedule and documents associated with that request;

(xxii) Letter of complaint from Digital Rights Ireland CLG to the DPC, dated 11 October 2018, and the associated mandate dated 9 October 2018;

(xxiii) Correspondence from the Inquiry Team to the DPO, dated 15 March 2019, notifying the DPO of the Inquiry Team's wish to conduct an interview;

(xxiv) Correspondence from the DPO to the Inquiry Team, dated 19 March 2019, confirming that the DPO was available to attend interview and seeking further information;

(xxv) Correspondence from the Inquiry Team to the DPO, dated 21 March 2019, regarding the voluntary interview;

(xxvi) Correspondence from the Inquiry Team to the DPO, dated 26 March 2019, responding to the DPO's request for further information;

(xxvii) Correspondence from the Department to the Inquiry Team, dated 4 June 2019, requesting an extension on the deadline for submissions on the Draft Inquiry Report;

(xxviii) Correspondence from the Inquiry Team to the Department, dated 6 June 2019, acceding to the Department's request for an extension to the deadline for submissions on the Draft Inquiry Report;

(xxix) The Department's submissions on the Draft Inquiry Report, dated 24 July 2019;

(xxx) Statement of the Secretary General, Department of Employment Affairs and Social Protection, submitted with the Department's submissions on the Draft Inquiry Report;

(xxxi) Statement of the DPO at the time under consideration in this Inquiry, dated 22 July 2019, and submitted with the Department's submissions on the Draft Inquiry Report; and

(xxxii) The Department's submissions on the Draft Decision, dated 29 March 2021.