

In the matter of the General Data Protection Regulation and the Data Protection Act 2018

DPC Case Reference: IN-21-7-3

In the matter of the Department of Social Protection

Decision of the Data Protection Commission pursuant to Sections 111 and 124 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Sections 110 and 123 of the Data Protection Act 2018

DECISION

Decision-Maker for the Data Protection Commission:

Dale Sunderland, Commissioner for Data Protection

9 June 2025



Data Protection Commission
6 Pembroke Row, Dublin 2, D02 X963, Ireland.

TABLE OF CONTENTS

A.	Introduction.....	5
B.	Legal Framework for the Inquiry and the Decision	5
a)	Identification of controller	6
b)	Legal basis for the Decision	6
C.	Factual background	7
a)	Previous investigation	7
c)	Commencement and scope of the Inquiry	7
d)	Material scope of the Inquiry	7
e)	Temporal scope of the Inquiry	9
i.	Processing in respect of facial matching of biometric facial templates	9
D.	Preliminary issue: Application of the GDPR and LED.....	15
a)	Material scope of the GDPR and LED	15
f)	Submissions made by the DSP.....	18
g)	Analysis	20
E.	ISSUE 1: ASSESSMENT OF MATTERS CONCERNING THE LAWFULNESS OF PROCESSING.....	24
a)	Overview of the Relevant Law.....	24
ii.	GDPR.....	24
iii.	Clear, precise and foreseeable lawful basis	27
Case-Law of the European Court of Human Rights.....	27	
Case-Law of the Court of Justice of the European Union.....	29	
Conclusion on the requirement to have a clear, precise and foreseeable lawful basis.....	31	
iv.	Necessity and proportionality	31
v.	Submissions of the DSP	34
vi.	Analysis.....	36
Clear, precise and foreseeable lawful basis	38	
Necessity and proportionality	42	
Special category data.....	45	
Lawful basis under other sections of the 2018 Act	46	
vii.	Finding 1	47
F.	ISSUE 2: ASSESSMENT OF MATTERS CONCERNING THE RETENTION OF PERSONAL DATA	48
a)	Overview of the Relevant Legal Provisions	48
viii.	Submissions of the DSP	48
ix.	Analysis.....	50
x.	Finding 2	51
G.	ISSUE 3: ASSESSMENT OF MATTERS CONCERNING TRANSPARENCY.....	51
a)	Overview of the Relevant Legal Provisions	52

xi.	Submissions of the DSP	53
xii.	Analysis	57
xiii.	Finding 3	57
H.	ISSUE 4: ASSESSMENT OF MATTERS CONCERNING THE REQUIREMENT TO HAVE UNDERTAKEN A DATA PROTECTION IMPACT ASSESSMENT	58
a)	Overview of the Relevant Legal Provisions	58
xiv.	Submissions of the DSP	63
xv.	Analysis	66
xvi.	Finding 4	66
I.	FINDINGS	67
J.	ORDER TO CEASE PROCESSING.....	68
K.	REPRIMAND.....	69
L.	DECISION ON ADMINISTRATIVE FINES	70
a)	Whether to impose an administrative fine	70
i.	Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them	71
	Taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them	72
	The nature of the infringements	76
	The gravity of the infringements.....	77
	The duration of the infringements	77
	Assessment of Article 83(2)(a).....	78
ii.	Article 83(2)(b) GDPR: the intentional or negligent character of the infringement	78
iii.	Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects	79
iv.	Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32	80
v.	Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor	80
vi.	Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.....	81
vii.	Article 83(2)(g) GDPR: the categories of personal data affected by the infringement	81
viii.	Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement	82
ix.	Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures.....	82
x.	Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42.....	82

xi.	Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.....	83
xii.	Decision as to whether to impose a fine	83
b)	Decision on the amount of the administrative fine	83
i.	Article 83(3) GDPR	83
ii.	Categorisation of the infringements under Articles 83(4)-(6) GDPR.....	87
iii.	Seriousness of the infringement pursuant to Articles 83(2)(a), (b) and (g) GDPR	87
iv.	Imposing an effective, dissuasive and proportionate fine	88
v.	Aggravating and mitigating circumstances.....	88
vi.	The relevant legal maximums for administrative fines	89
vii.	Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness.....	90
	Effectiveness.....	90
	Dissuasiveness	90
	Proportionality.....	90
M.	SUMMARY OF ENVISAGED ACTION.....	91
N.	RIGHT OF APPEAL	92

A. Introduction

1. This document (“**the Decision**”) is a decision made by the Data Protection Commission (“**the DPC**”) in accordance with sections 111 and 124 of the Data Protection Act 2018 (“**the 2018 Act**”). The DPC makes this Decision having considered the information obtained in the own volition inquiry IN-21-7-3 (“**the Inquiry**”) pursuant to sections 110 and 123 of the 2018 Act.
2. The Department of Social Protection (“**the DSP**”) was provided with a draft decision (“**the Draft Decision**”) on this inquiry on 29 November 2023 to give the DSP an opportunity to make any submissions the DSP deemed necessary. The DSP responded to the DPC’s Draft Decision on 21 February 2024. The DPC finalised the Decision taking into account the DSP’s submissions dated 21 February 2024.
3. This Decision contains corrective powers under section 127 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. The DSP will be required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on the DSP in accordance with section 133 of the 2018 Act.

B. Legal Framework for the Inquiry and the Decision

4. The GDPR is the legal regime governing the processing of personal data in the European Union (“**EU**”). As a regulation, the GDPR is directly applicable in member states of the EU. The GDPR is given further effect in Irish law by the 2018 Act. Under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on foot of a complaint or of its own volition.
5. 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, as per section 105(1) of the 2018 Act.
6. Part 5 of the 2018 Act transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (“**the LED**”). Part 5 of the 2018 Act is the legal regime covering the processing of personal data that falls within the material scope of Article 2 LED and section 70 of the 2018 Act. Under Chapter 3 of Part 5 of the 2018 Act, the DPC has the power to commence an inquiry on foot of a complaint or of its own volition.

7. Section 123(1) of the 2018 Act provides that the DPC may, for the purpose of section 122(4)(e), 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 Part 5 of the 2018 Act.

a) Identification of controller

8. The DSP is a department of state, established pursuant to the Constitution of Ireland and the Ministers and Secretaries Act 1924, as amended. The DSP is principally located at Áras Mhic Dhiarmada, Store Street, Dublin 1.

9. The DPC accepts that the DSP is the controller for the purposes of Article 4(7) GDPR and the 2018 Act as stated in the DSP's submissions to the Inquiry on 17 September 2021.¹

b) Legal basis for the Decision

10. The decision-making process for the Inquiry which applies to this case is provided for under sections 111 and 124 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. This function is performed by a member of the DPC as defined in section 15 of the 2018 Act, acting as decision-maker. The decision-maker is required to assess all of the materials and submissions gathered during the Inquiry and any other materials considered to be relevant in the course of the decision-making process. A full schedule of all documentation considered for the purpose of the preparation of this Decision is appended.

11. For the purposes of this Decision, the DPC has fully considered all of the information and documentation provided by the DSP – all correspondence and enclosures sent by the DSP to date, as well as all documents and resources referred to within all of the information and documentation submitted. The DSP has been provided with an opportunity to consider and make submissions in relation to all steps of the Inquiry to date and has been facilitated to do so.

12. Having considered the information obtained in the Inquiry, the DPC is satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout.

¹ Appendix D.2.2, p16, 18.

C. Factual background

a) Previous investigation

13. The legal basis for the processing of the personal data of the SAFE registration process (“**SAFE registration**”) and Public Service Cards (“**PSC**”) were subject to a previous investigation by DPC under section 10(1A) of the Data Protection Acts 1988-2003. An enforcement notice issued by DPC on 6 December 2019. The DSP issued proceedings by way of an appeal to the Circuit Court. The matter was settled and the appeal was withdrawn by the DSP. A joint agreement and final investigation report (“**the Final Investigation Report**”) were published on 10 December 2021.²

c) Commencement and scope of the Inquiry

14. A Notice of Commencement of Inquiry (“**Commencement Notice**”) issued to the DSP on 20 July 2021. The Commencement Notice set out that the Inquiry would examine the processing of personal data in connection with the use or application of biometric facial templates (and associated facial matching technologies) in the SAFE 2 registration process (“**SAFE 2 registration**”) and in connection with the associated issuing of PSCs.³

15. The Commencement Notice also indicated that the Inquiry would be particularly concerned with the requirement for such personal data to be processed lawfully, fairly and in a transparent manner in relation to data subjects.

d) Material scope of the Inquiry

16. Paragraph 177 of the Final Investigation Report stated that processing of personal data in respect of facial matching of biometric facial templates (also referred to as “arithmetic templates”) would be the subject of a separate report. Accordingly, the purpose of this present Inquiry is to examine the processing of biometric facial templates in SAFE 2 registration as it is currently carried out by or on behalf of the DSP and by reference to the legislative framework presently in force, that is pursuant to the GDPR and the 2018 Act.

17. The Commencement Notice stated that the scope of the Inquiry would examine and assess the DSP’s compliance with Articles 5, 6, 9, 12 to 14, and 35 GDPR, and, where applicable, relevant provisions of the 2018 Act which relate to or give further effect to those Articles of the GDPR. It also stated that should the DSP indicate in its responses

² For completeness, the DPC notes that the DSP set out their account of the factual background in their submissions on the Draft Decision as set out at Appendix D.10.1 at p91-97.

³ Appendix D.1.1, p8-9.

to the Inquiry that any aspect of the processing of biometric facial templates during SAFE 2 registration fell within the scope of Part 5 of the 2018 Act, the DPC, having considered the information furnished by the DSP, may extend the scope of the Inquiry to include relevant provisions of Part 5 of the 2018 Act.

18. In the DSP's response to the Commencement Notice,⁴ it stated that, without prejudice to other grounds that are relevant, the DSP asserts that Part 5 of the 2018 Act, which transposes the LED, provides a legal basis for its processing of biometric data together with Article 6(1)(e) GDPR.
19. On 21 March 2022, the DPC wrote to the DSP with further queries, which were responded to on 6 May 2022.⁵ Additionally, on 30 March 2022, authorised officers of the DPC attended the premises of the DSP at Goldsmith House, Pearse St, Dublin 2 and D'Olier House, D'Olier Street, Dublin 2 in order to carry out an inspection under Part 6 of the 2018 Act of SAFE 2 registration. In the course of that visit, the DPC posed a number of questions to the DSP. On 9 June 2022, the DSP responded to those queries.⁶
20. The DPC prepared an inquiry issues paper ("**the Inquiry Issues Paper**") to document the relevant facts established and the issues that fell for consideration for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry. The DPC furnished the DSP with the Inquiry Issues Paper on 5 August 2022 and invited submissions on any inaccuracies and/or incompleteness of the facts. The Inquiry Issues Paper stated that, if Part 5 of the 2018 Act was found to apply to the relevant processing, in addition, sections 71(2), 71(1)(e), 84 and 90 of the 2018 Act would also fall for consideration.
21. In light of the responses and submissions received from the DSP, as set out in the Inquiry Issues Paper, a preliminary matter arose:

*"As a preliminary matter, the DPC must make a determination as to whether the GDPR/2018 Act (excluding Part 5) applies and/or whether Part 5 of the 2018 Act (giving effect to the LED) applies to the processing under examination i.e. the processing of biometric facial templates by way of facial matching during the SAFE registration process."*⁷

22. Additionally, the relevant issues to be determined as part of the Inquiry were:⁸
 - i. An examination of the lawfulness of processing;

⁴ Appendix D.2.2, p25-26.

⁵ Appendix D.3.1 and D.3.2.

⁶ Appendix D.4.1.

⁷ Appendix D.6.2, p17.

⁸ Appendix D.6.2, p17-18.

- ii. An examination of compliance with provisions regarding retention of personal data in the GDPR and 2018 Act;
- iii. An examination of compliance by the DSP with transparency provisions of the GDPR and 2018 Act; and
- iv. The DSP's compliance with the requirement to have undertaken a DPIA.

In the course of examining those issues, the DPC has had regard to the relevant provisions of the Social Welfare Consolidation Act 2005 (“**the 2005 Act**”) relied upon by the DSP.

23. The DSP provided submissions on the Inquiry Issues Paper on 17 September 2022⁹ and further submissions on the Draft Decision on 21 February 2024. The DPC has had full regard to those submissions and the DPC has reached conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. These infringements and corrective powers are set out in this Decision.

e) Temporal scope of the Inquiry

24. The temporal scope of this Inquiry includes processing by the DSP during the period between 25 May 2018 (the date when the GDPR became applicable and the provisions of the 2018 Act relevant to this Inquiry were commenced) and the commencement of this Inquiry on 20 July 2021 (“**the temporal scope**”).

i. Processing in respect of facial matching of biometric facial templates

25. SAFE, referring to “Standard Authentication Framework Environment”, is the standard used by the DSP to establish and verify a person’s identity.¹⁰ The DSP’s “Comprehensive guide to SAFE Registration and the Public Services Card” states¹¹ that SAFE Registration allows the DSP to be sure that:

- a. the person using its service is the person they claim to be,
- b. that nobody else is using that person’s identity for the purpose of claiming a payment of service,

⁹ Appendix D.7.1.

¹⁰ The DSP states in Appendix 3 to their Submissions of 24 February 2024 that the term “SAFE registration” is a term understood and used across the Irish public service to describe the identity authentication process carried out by the DSP. The DSP further states that the specifications for SAFE were established under the aegis of an Interdepartmental Group jointly chaired by the DSP and the Department Finance.

¹¹ Appendix D.5.1, p8.

- c. that the person is not claiming another payment or using another service under a different identity and in addition,
 - d. to minimise the requirement for people to provide the same identity information over and over again when accessing different services.
26. The SAFE standard has four levels of identification, ranging from “SAFE 0” to “SAFE 3”. SAFE 2 registration is used by the DSP to authenticate the identity of:
- a. Persons resident in the State who apply for a Personal Public Service Number (“PPSN”).
 - b. Persons who apply for a PSC.
 - c. Persons who make a claim for a social welfare benefit.
 - d. Persons in receipt of a social welfare benefit who are requested to satisfy their identity to the Minister.

SAFE 2 registration refers to, as stated by the DSP, the provision of a “substantial assurance” as to the identity of a data subject, which is the DSP’s minimum authentication level for issuing a PSC.¹² It should be noted that because SAFE 2 Registration denotes one level of authentication within the broader SAFE standard devised by the DSP, the terms SAFE registration and SAFE 2 registration are often used interchangeably, alongside other similar terminology. To avoid confusion, this Decision shall primarily use the term SAFE 2 registration to describe the processing of personal data in connection with the use or application of biometric facial templates and associated facial matching technologies as outlined in the commencement notice.

27. A PSC is required to access a wide range of public services provided by the DSP. Specified bodies,¹³ other than the DSP, use the PSC to verify the identity of data subjects wishing to access public services, save that a data subject is not required to obtain a PSC to access public services from a specified body unless this requirement is set out in legislation. A data subject who wishes to avail of a PSC attends at a DSP Intreo or SAFE registration centre where their facial image is captured by photograph. A biometric template is then generated from that photograph. That biometric template is compared to all other biometric templates generated from all other photographs taken of the facial images of data subjects who have previously had their facial image captured by the DSP.¹⁴ No photographs are currently submitted or sourced from any other public body, office or agency for the purpose of SAFE 2 registration.¹⁵

¹² Appendix D.5.1, p8.

¹³ As designated under Schedule 5 SWCA 2005 as amended.

¹⁴ Appendix D.2.2, p2-3.

¹⁵ Appendix D.2.2, p8.

28. The Cogent Facial Image Matching System (“**CFIMS**”) feature extraction (also referred to as “template generation” and “template creation”) analyses the facial image and generates a numerical representation of the face. This numerical representation is the biometric template that then represents the features and characteristics found on the face. The templates are processed using a matching algorithm which compares biometric templates to compute a matching score. In a facial recognition context, this score represents a measurement of the likelihood that two separate images refer to the same person. CFIMS compares the template it creates from a new facial image with the other templates already held by the DSP. This is referred to as “one-to-many matching”.
29. Where a data subject already holds a PSC and seeks to renew it, they can update the photograph of their facial image online (up until March 2020, they could also do so by post).¹⁶ This is in turn subject to a similar process, whereby the template is subjected to one-to-many matching and in addition is compared against the previous template held in relation to the same data subject. That is, the new template is matched against the previous template. This is referred to as “one-to-one matching”.
30. The matching score created is then referenced against certain threshold values which are set within the CFIMS system:
- i. Lower threshold: If the matching score is below this value, this means that no biometric template of a facial image already held by the DSP within the CFIMS system has been found to be sufficiently similar to the biometric template of the new facial image to raise concerns that the two facial images may be of the same person.
 - ii. Middle threshold: If the matching score is between the lower and upper threshold values, this means that another biometric template of a facial image already held by the DSP has been found that is sufficiently similar to the new biometric template to raise the question as to whether the facial images are of the same person.
 - iii. Upper threshold: If the matching score is above this value, this means that another biometric template of a facial image already held by the DSP has been found that is so similar to the biometric template of the new facial image photograph that there is a strong possibility that the facial images are of the same person.¹⁷
31. In the case of new registrations, where a matching score is in the middle threshold range or upper threshold range for the one-to-many matching exercise or the one-to-one matching exercise, the case is referred to an officer of the DSP within its Client Identity Services (“**CIS**”) division for human evaluation. In the case of renewals, the

¹⁶ Appendix D.2.2 p2-3.

¹⁷ Appendix D.2.2, p4.

expected result in a one-to-one match being that the score would be in the upper threshold range, such cases are not referred to an officer for evaluation. However, where the one-to-one match score in a renewal case is in the lower or middle threshold ranges, the officer examines the facial images involved, via the CFIMS user interface, and assesses whether there is a question as to the identity of the person concerned. If the officer forms the view that there is a legitimate question as to the identity of the person concerned, the case is referred to the DSP's Special Investigations Unit ("SIU"). If the officer is satisfied that there is no evidence of suspected identity fraud, SAFE 2 registration of the individual is completed.¹⁸

32. 35% of new SAFE 2 registration cases are referred for human evaluation because the matching score is in the middle threshold range or the higher threshold range. On renewal, in relation to one-to-one matching, 95% of PSC renewal cases are referred for human evaluation because the matching score is in the lower threshold range or the middle threshold range, and in relation to one-to-many matching, 45% of PSC renewal cases are referred for human evaluation because the matching score is in the middle threshold range or the higher threshold range.¹⁹ The DSP in their submissions²⁰ states that of the 35 staff assigned to CIS, 20 officers are assigned to the main adjudication team which carries out human adjudications daily; 7 are assigned to the escalation team, who deal with cases that are escalated from the main adjudication team and general system administration tasks; with 8 officers assigned to the assistance team who are only called upon to carry out human adjudications when the volume of cases on hand increases, so as to avoid delays to PSCs issuing to applicants. The DSP states that 30 staff are involved in the facial image matching process and that none of these staff have access to the biometric templates.

33. The DPC observes that for renewals, if the system were working as the DSP intended it to, every new image should have a high matching score with the previous photo of that person on the one-to-one matching. The statistics outlined above show a low rate of successful matches between new templates and the previous template on renewal (one-to-one). Similarly, those statistics show that nearly half of renewals potentially match the photograph of someone else (one-to-many). In itself, those statistics show that human intervention is needed in a high number of cases.

34. The DSP submits²¹ that the high number of cases referred for human evaluation does not reflect a failure in the current system. Rather the DSP submits that high numbers of cases referred to human evaluation demonstrates the DSP's commitment to ensuring

¹⁸ Appendix D.7.1 at 8.

¹⁹ Appendix D.4.1

²⁰ Appendix D.10.1 at 107 paras 14-20.

²¹ Appendix D.10.1 at 108 and 109 paras 21-30.

that biometric processing is used properly. The DSP submits that biometric processing is essential to narrow down the number of images which would otherwise require evaluation. The DSP notes that other forms of biometric processing, such as iris scanning and fingerprint matching, are more intrusive forms of biometric processing and it was on that basis that the DSP chose facial matching. The DSP explains that an individual's face changes with age and as a result the DSP must obtain a new facial match every 10 years. The DSP states that it will review its thresholds for human evaluation and adjust thresholds based on its experience since the introduction of facial matching.

35. Biometric templates are stored within the CFIMS database on the DSP's IT infrastructure. They are retained for the lifetime of the person concerned, plus 10 years.²² The biometric templates are not shared with any organisation or body; they are processed solely by the DSP for the purpose of identity authentication. The DSP does not carry out facial image matching on behalf of any other bodies or agencies. No other body or agency carries out facial image matching on behalf of the DSP.²³
36. By 15 September 2021, the DSP held photographs and biometric templates in respect of 3,465,745 data subjects whose identity had been "*substantially assured*" by way of SAFE 2 registration. In addition, the DSP held photographs and biometric templates in respect of 22,356 people who had begun SAFE 2 registration but had not completed it. At 15 September 2021, the total overall number of data subjects in respect of whom the DSP held photographs and biometric templates was 3,488,101.²⁴
37. At 15 September 2021, of the 3,465,745 people who had undergone SAFE 2 registration, 13,103 of these were under 18 and 3,452,642 were 18 or over. As of 15 September 2021, a total of 3,625,597 photographs had been used to generate a biometric template. This included templates created in respect of SAFE 2 registrations, PSC renewals and those awaiting PPSNs. The difference between the number of photographs (3,625,597) and the number of SAFE 2 registrations (3,465,745) is 159,852. The DSP submits that:

*"This difference can be accounted for as 135,592 PPSNs have more than one photo (and template) associated with them, and the Department holds photographs of 22,356 people who have not yet completed the SAFE process."*²⁵

²² Appendix D.2.2 at 6.

²³ Appendix D.3.2 at 12 and D.7.1 at 2.

²⁴ Appendix D.2.2 at 9.

²⁵ Appendix D.2.2 at 9.

38. From January 2018 to September 2021,²⁶ the number of times the facial matching process was carried out in each year was:

- a. 403,567 (2018)
- b. 310,305 (2019)
- c. 170,595 (2020)
- d. 107,609 (2021)

39. As previously noted, the following categories of persons have undergone, and continue to undergo SAFE 2 registration in the State since 25 May 2018:

- a. Persons resident in the State who apply for a PPSN;
- b. Persons who wish to acquire a PSC;
- c. Persons who make a claim for a social welfare benefit; and
- d. Persons in receipt of a social welfare benefit who are requested to satisfy the Minister for Social Protection as to their identity.²⁷

40. In its Comprehensive Guide to the PSC, the DSP states:

“[A]ll recipients of welfare services and payments in Ireland have or will be asked to complete the SAFE registration process (some exceptions may be made for example in respect of people with profound disabilities). Failure to complete a SAFE registration process when requested can result in refusal of a new welfare claim or withdrawal of an existing payment or benefit.

The Department of Employment Affairs and Social Protection makes it clear to customers in receipt of welfare payments or entitlements that they do need to register to SAFE 2, in accordance with the relevant legislative provisions, to access or to continue to access those payments/entitlements.” (emphasis added)²⁸

41. In addition, a person who is entitled to free travel can use their PSC as a travel pass on public transport. If a person who has not already undergone SAFE 2 registration qualifies for free travel, they are invited by the DSP to attend for SAFE 2 registration at

²⁶ Appendix D.2.2 at 11.

²⁷ Appendix D.2.2 at 12.

²⁸ Appendix D.5.1 at 10.

an office of the DSP. If a person who already has undergone SAFE 2 registration qualifies for free travel, a new free travel PSC issues automatically to that person.²⁹

42. The biometric template is not stored on the PSC, nor is it shared with other specified bodies. The provider of the facial matching software is Thales DIS (UK & Ireland) (formerly Gemalto). The provider is neither a controller nor a processor in respect of the processing of biometric data in connection with SAFE 2 registration.³⁰

43. In respect of cases of suspected identity fraud referred for investigation, where the referral arose as a result of an officer in CIS having decided that there was a question as to a person's identity, 73 cases of suspected identity fraud were referred to the SIU of the DSP between 25 May 2018 and 21 March 2022. There have been 20 criminal convictions for identity fraud arising out of the processing of biometric data in relation to SAFE 2 registration between 25 May 2018 and 21 March 2022. The total overall number of criminal convictions for identity fraud, arising out of the processing of biometric data in relation to SAFE 2 registration since the system was introduced, is 48.³¹

D. Preliminary issue: Application of the GDPR and LED

a) Material scope of the GDPR and LED

44. As a preliminary matter, as noted above, the DPC must make a determination as to whether the GDPR and 2018 Act (excluding Part 5) applies or whether Part 5 of the 2018 Act (giving effect to the LED) applies to the processing under examination – that is, the processing of biometric facial templates by way of facial matching during SAFE 2 registration.

45. In conducting this assessment and determination, regard will be had, *inter alia*, to the stated purposes of the processing of personal data by the DSP, i.e. whether the processing of personal data in the form of facial matching of biometric facial templates is conducted for purposes covered by Article 2(2)(d) GDPR, which provides that:

“This Regulation does not apply to the processing of personal data ... by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”

²⁹ Appendix D.2.2 at 12.

³⁰ Appendix D.2.2 at 18.

³¹ Appendix D.3.2 at 6-7.

46. The LED is a *lex specialis* that provides specific rules with regard to the processing of personal data for such purposes. The LED is transposed into Irish law by Part 5 of the 2018 Act which, as set out in section 70 therein, applies:

“...to the processing of personal data by or on behalf of a controller where the processing is carried out—

(a) for the purposes of—

(i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or

(ii) the execution of criminal penalties,

and

(b) by means that—

(i) are wholly or partly automated, or

(ii) where the personal data form part of, or are intended to form part of, a relevant filing system, are not automated.”

47. “Controller”, for the purposes of Part 5, is defined in section 69(1) as:

(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or

(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated—

(i) by that law, or

(ii) in accordance with criteria specified in that law”;

48. “Competent authority”, for the purposes of Part 5, is defined in section 69(1) as including:

“(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or...”

49. Two criteria must be fulfilled for the LED, as incorporated by Part 5 of the 2018 Act, to apply to processing of personal data. First, the processing must be conducted by or on behalf of a “controller” as defined in section 69 of the 2018 Act. Secondly, pursuant to section 70 of the 2018 Act, the processing must be carried out for law enforcement purposes, that is the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or the execution of criminal penalties.
50. In *Puskar v Finance Directorate of the Slovak Republic*,³² the Court of Justice of the European Union (“CJEU”) considered the scope of the Data Protection Directive,³³ specifically the directive’s non-application to processing operations concerning the activities of the State in areas of criminal law.³⁴ This case considered the inclusion of an individual’s name on a list of persons that the Finance Directorate considered “front-men” in company director roles. The data at issue were processed for the purpose of collecting tax and combating tax fraud. However, that data could be used in criminal proceedings if infringements were identified. The Court considered the purposes of the processing and held that the data were not collected “for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law”.³⁵ On that basis, the criminal law exclusion was not applicable, and the Data Protection Directive was held to apply to that processing.
51. In the *Puskar* case the CJEU adopted a strict interpretation of the scope of the criminal law exclusion in the Data Protection Directive. For that exclusion to apply, it was not sufficient that the data could potentially be used in criminal proceedings. Rather, the data must have been collected for the specific purpose of the pursuit of criminal proceedings. A similarly strict interpretation of the application of the LED and section 70 of the 2018 Act is warranted in the light of the principle that exceptions to the application of the GDPR must be interpreted strictly.³⁶ Thus, processing is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences only if the controller’s reasons for the processing specifically reflects one or more of those purposes. It is not sufficient that the data could potentially also be used

³² Case C-73/16, *Peter Puskar v Finance Directorate of the Slovak Republic*, judgment of 27 September 2017 (ECLI:EU:C:2017:725).

³³ Directive 95/45/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³⁴ That exclusion is provided for in Article 3(2) of the Directive.

³⁵ At paragraph 40.

³⁶ See *VS v Inspektorata kam Visshia sadeben savet*, judgment of 8 December 2022 Case C-180/21, (ECLI:EU:C:2022:967).

for law enforcement purposes if those purposes did not form part of the controller's specific reasons for processing.

f) Submissions made by the DSP

52. SAFE 2 registration entails the processing of biometric data to authenticate identity. A biometric template is generated from a photograph of the data subject's face and compared to existing templates to verify that the individual was not previously authenticated under a different identity.³⁷

53. Article 6(1)(e) GDPR states that processing is lawful if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In its submissions to the Inquiry, the DSP stated that this represents the lawful basis of the personal data processing and that this is laid down in law in sections 241, 242, 247C and 263B the Social Welfare Consolidation Act of 2005.³⁸ The DSP also cites sections 38(1), 41, 45, 46, 47 and 49 of the 2018 Act and Article 9(2)(b) and (g) GDPR as applicable to the lawful basis for the processing of personal data.³⁹

54. According to these provisions, the DSP can:

- a. Request to take a photograph of an individual (section 241(1C))
- b. Retain these images in electronic form (section 241(1D))
- c. Request that an individual attends an office to allow collection of data (sections 247C and 263B)

55. The DSP considers itself a competent authority and data controller as defined in section 69(1)⁴⁰ and that biometric data processing is included in the definition of processing as per section 70.⁴¹ The DSP identifies the prevention, investigation, detection and prosecution of criminal offences as set out in sections 250 and 251 of the 2005 Act as the purposes of the processing.⁴²

56. In its submissions, the DSP states:

*"In part 3.2.7 of its Final Report, where the DPC considered the provisions contained in s 263B, the DPC accepted that the provisions in s.263B correspond to the SAFE 2 registration requirements"*⁴³

³⁷ Appendix D.2.2 p25.

³⁸ Appendix D.2.3 p42.

³⁹ Appendix D.2.2 p28-30.

⁴⁰ Appendix D.2.2 p16 and D.10.1 p13-14.

⁴¹ Appendix D.2.2 p17.

⁴² Appendix D.2.2 p16-17.

⁴³ Appendix D.2.2 p26.

57. With regard to Part 5 of the 2018 Act, the DSP also has stated that:

“It is the Department’s position that the processing of biometric data carried out as part of SAFE registration falls within Part 5 of the 2018 Act.

Firstly, under Section 251 of the Social Welfare Consolidation Act (2005) (as amended) it is a criminal offence for a person to knowingly make any representation or knowingly conceal any material fact for any purpose connected with the Act. A person found guilty of an offence is liable on conviction in a court to penalties including imprisonment for a term of up to 3 years.

Section 250 of the SWCA 2005 provides for the appointment of Social Welfare Inspectors (SWIs) and deals with the powers of a SWI. These powers include, inter alia, the power to: investigate and report to the Minister on any claim for or in respect of benefit or any queries relating to that benefit, and for an application and use of a PPSN; enter premises; examine records; be accompanied by a Garda when carrying out his functions.”

58. The DSP’s submissions on the Draft Decision restate its position that the purpose of SAFE 2 registration is the detection and prevention of fraud. The DSP cites the following sections of the 2005 Act in support of its position: section 2(1), section 241(1)(c), section 241(1C), section 241(1D), sections 247C(1)-(2), section 247C(3)(c), section 247C(4)(a), section 251(1), section 262(2A), section 262(A) section 263(1), section 263(1C), section 263B(1)(c), section 263B(2) and section 272(1).⁴⁴ The DSP submits that these provisions provide the legislative purpose of SAFE 2 registration. The DSP also references the fact that sections 251-274 of the 2005 Act are positioned in Chapter 4 of the 2005 Act which is entitled “*Offences, Miscellaneous Control Provisions and Proceedings*”.⁴⁵ The DSP states that the provisions in Chapter 4 of the 2005 Act are designed to support the prevention, detection, investigation and prosecution of the criminal offences created by and set out in sections 251, 262A and 263 of that Chapter. Further, the DSP provides extracts from Oireachtas debates relating to the issue of welfare fraud.⁴⁶

59. The DSP’s position is that, without prejudice to its view that Part 5 of the 2018 Act applies to the processing, that it also has a relevant lawful basis under the GDPR to conduct SAFE 2 registration.

⁴⁴ Appendix D.10.1, p13-14.

⁴⁵ Appendix D.10.1, p14.

⁴⁶ Appendix D.10.1, p14-16.

g) Analysis

60. It is accepted that the DSP is authorised under the provisions set out in paragraph 57 to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State.

61. The processing of personal data carried out in relation to SAFE 2 registration is carried out for the purposes of identity authentication in order for the applicant to be issued with a PSC to access services provided by the DSP. Where an applicant does not submit to such processing, the PSC does not issue. This in turn means that a person cannot access the relevant DSP services, including accessing welfare payments, as a PSC is a prerequisite to avail of those services. The DSP submits that all of this processing is covered by Part 5 of the 2018 Act, as it is carried out for the purposes of welfare fraud prevention.

62. The DSP's leaflet "Safe Registration and your Personal Data", which is provided to applicants during SAFE 2 Registration states:

"At SAFE registration, you provide personal data to verify your identity. Once you verify your identity to the substantial level required, a Public Services Card (PSC) will be issued to you.

*The photograph used for SAFE registration is **also** processed using facial matching software to detect and prevent identity fraud."* (emphasis added)

63. The DSP's Comprehensive Guide to SAFE Registration and the Public Services Card states:

"SAFE 2 = Substantial assurance (the minimum authentication level for issuing a Public Services Card)"

64. It also states:

"The Department of Employment Affairs and Social Protection makes it clear to customers in receipt of welfare payments or entitlements that they do need to register to SAFE 2, in accordance with the relevant legislative provisions, to access or to continue to access those payments/entitlements."

And:

"SAFE 2 identity verification is currently required for –

Access to Social Welfare Services (including Child Benefit and Treatment Benefits)"

65. In 2021, the DSP published a report entitled “Public Service Identity Management Framework Cost Benefit Analysis”.⁴⁷ Section 3.2.2 of the report states that “...*The purpose of the PSC is to act as a physical token that can be presented by a person attesting to the fact that their identity has been authenticated using SAFE, and in this way enables them to gain access to public services more efficiently.*

[...]

The electronic information encoded on the PSC as a result of the SAFE 2 process is used as a mechanism to support some DSP service transactions. This includes payment of Welfare benefits such as pensions, jobseekers’ payments, carers, disability payments and child benefit made at Post Offices. Where a customer presents with a PSC, the An Post agent can swipe the magnetic strip on the back of the card through a card reader.”

66. On the basis of a consideration of all of the submissions made and an examination of the process and its purposes, it is clear that the DSP utilises SAFE 2 registration in order to authenticate the identity of a data subject for the purposes of verifying their entitlement to a PSC or renewing a PSC *per se* – that is, as part of the process to ensure that the Minister can be satisfied as to the identity of a person, as required under the relevant legislative provision.⁴⁸ This is in circumstances where such processing is a prerequisite to the issuance of a PSC, so that in turn the data subject can access welfare payments to which they may be entitled. Verifying that an individual is entitled to the receipt of a welfare payment is not a law enforcement purpose, it is an administrative check that an individual has an entitlement to receive certain statutory benefits.

67. The DSP in its submissions on the Draft Decision objects to the use of the term “administrative check”. The DSP states that the biometric processing in SAFE 2 registration is for the purpose of carrying out the Minister’s statutory function of authenticating identity. The processing of biometric data as part of SAFE 2 registration is a process by which the biometric facial image of an individual applying for or renewing a PSC is checked against existing facial images held by the DSP. This processing, by itself, does not authenticate the identity of the individual and accordingly is most appropriately described as an administrative check.⁴⁹

⁴⁷ “The SAFE-PSC-MyGovID Framework for Public Service Identity Management: A Cost Benefit Analysis” (Department of Social Protection, November 2021) <<https://assets.gov.ie/203598/e1d8ee32-ed9c-43dd-8034-6c7bf3a0bb74.pdf>>, (accessed 7 April 2025).

⁴⁸ Appendix D.2.2, p25.

⁴⁹ The term “administrative check” refers to a non-criminal investigation or review conducted by public authorities to monitor compliance with laws or regulations. The Publications Office of the EU defines “administrative check” within its controlled vocabularies, indicating its recognized usage in EU documentation: “administrative check”, European Vocabularies, (Publications Office of the European Union), <https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http%3A%2F%2Fpublications.europa.eu%2Fresource%2Fauthority%2Ffd_300%2F000171&utm>, (accessed 7 April 2025).

68. The DSP also refers cases to the SIU in some instances following a matching score. The biometric template is not forwarded to the SIU or to An Garda Síochána. The referral to SIU only takes place following human evaluation. Thus, while the biometric processing will identify possible facial matches for human review, it is the SIU that determines if further investigation and/or referral to An Garda Síochána is warranted. The biometric processing is disconnected from any criminal investigation. It is not the direct trigger for an investigation, and it is not included in the file for an investigation or prosecution either internally or externally. Therefore, following the CJEU case-law outlined above, the DPC is satisfied that Part 5 of the 2018 Act (giving effect to the LED) does not apply to SAFE 2 Registration. This is not to say that Part 5 of the 2018 Act does not apply to the processing of personal data by the SIU. Such an assessment is beyond the scope of this Decision.
69. On the basis of the case-law outlined in paragraph 50, the fact that the biometric processing could subsequently be used to trigger criminal prosecutions does not bring the processing within the scope of the LED. In this regard, two paragraphs from the *Puskar* judgment are worth extracting in particular:

“39 In the case in the main proceedings it is apparent from the order for reference that the data at issue are collected and used for the purpose of collecting tax and combating tax fraud. Subject to the determinations to be carried out in that regard by the referring court, however, it does not appear that the processing of that data has as its object public security, defence or State security.

40 Besides, even if it does not appear to be excluded that that data may be used in criminal proceedings which may be brought, in the event of an infringement in the field of taxation, against certain persons whose names are included in the contested list, the data at issue in the case in the main proceedings do not appear to have been collected for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law” (emphasis added)

70. The example in those paragraphs is analogous with the processing in SAFE 2 registration, particularly as regards the distinction drawn by the emphasised text between the purposes of combating tax fraud and pursuing criminal proceedings. SAFE 2 registration relates to the issuance of a PSC, as outlined above. According to the DSP, SAFE 2 registration also contributes to the identification of cases of welfare fraud and the possible need for criminal proceedings. Applying the logic in the *Puskar* case, the identification of welfare fraud is distinct from the specific purpose of the pursuit of criminal proceedings or activities relating to criminal law. The processing for SAFE 2 registration is even further removed from criminal proceedings than the example in the *Puskar* case. In that case, the data in question may have been used in criminal

proceedings. By contrast, the biometric data processed by the DSP for SAFE 2 registration is not used in an actual investigation into a suspected offence. The processing of that data triggers human evaluation, which in turn can lead to the referral of a file to the SIU. Therefore, biometric data are not processed for the specific purpose of pursuing criminal proceedings. As outlined above, the data are processed for the purposes of authenticating identity to issue a PSC. The fact that the process may flag a need for human evaluation as a further step in the authentication process is insufficient to bring the biometric processing within the scope of the LED or Part 5 of the 2018 Act – biometric data are not processed from the point of human evaluation onwards. Were it to be the case that further processing of biometric data was subsequently undertaken by the SIU in the investigation of a suspected fraudulent application, for example, then such processing would likely fall within the scope of Part 5 of the 2018 Act. However, such an assessment is beyond the scope of this Decision.

71. The DSP's submissions on the Draft Decision state that the DPC, in relying on the case of Puskar,⁵⁰ takes insufficient regard to the fact that this case was decided under the Data Protection Directive 1995. The DSP states that the scope of activities under the Directive was narrower than under the LED⁵¹ and that, in applying Puskar, the DPC placed an over-emphasis on the criminal prosecution aspect of the function. The DSP submits that facial matching is an immediate trigger for human evaluation for the purpose of detection of a crime, which the DSP further submits, is a separate purpose under the LED. The DSP cites *V.S.*⁵² as an authority for the position that each of the LED's purposes including the prevention, investigation, detection or prosecution of crime can be specific and distinct purposes. The DSP also cites the Opinion of Advocate General Campos Sanchez Bordonada in the unrelated *VS*⁵³ case, in which one of the questions referred to the CJEU concerned the interpretation of the purposes listed in Article 1(1) of the LED.

72. The DPC accepts that under the LED personal data can be processed for separate purposes, however, the DPC notes that the decision in *VS* related to personal data processed for the purposes of investigating a crime in the first instance and then subsequently to use the personal data collected for the separate purpose of prosecuting a crime. The DPC further notes that in *VS* the personal data was processed for separate law enforcement purposes. In contrast, the biometric processing in SAFE 2 registration is not processed for a law enforcement purpose. As outlined, two cumulative criteria

⁵⁰ Case C-73/16 *Puskar*.

⁵¹ Article 1(1) of the Law Enforcement Directive and section 70(1)(1) Data Protection Act 2018. The CJEU in the case C-205/21, paragraphs 39 to 63.

⁵² See *V.S. v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, judgement of 26 January 2023, Case C-205/21, (ECLI:EU:C:2023:49).

⁵³ Case C-180/21 *VS*

must be fulfilled in order for processing to fall within the scope of the LED and Part 5 of the 2018 Act. For the reasons already explained, SAFE 2 registration only fulfils one of these criteria. Therefore, the DSP's submissions in this regard are based on a straightforward misinterpretation of the interplay between the GDPR and the LED.

73. Thus, the biometric data used in SAFE 2 registration are not processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security by a competent authority. As such, that processing falls within the material scope of the GDPR, and outside the scope of the LED and Part 5 of the 2018 Act.

E. ISSUE 1: ASSESSMENT OF MATTERS CONCERNING THE LAWFULNESS OF PROCESSING

74. As set out in the Inquiry Issues Paper, the DPC must now determine whether the DSP has a lawful basis for the collection of biometric data for the purposes of facial matching during SAFE 2 registration under the GDPR.

75. With regard to the GDPR, the lawful basis for the GDPR processing will be examined having regard to:

- i. Article 5(1)(a) GDPR;
- ii. Article 6(1)(e) GDPR; and
- iii. Article 9(2)(b) and (g) GDPR.

a) Overview of the Relevant Law

76. This section summarises the provisions of the GDPR applicable to the DSP's processing. It then summarises relevant aspects of EU and ECHR case-law.

ii. GDPR

77. Article 5(1)(a) GDPR provides that:

Personal data shall be:

"... processed lawfully, fairly and in a transparent manner in relation to the data subject" ("lawfulness, fairness and transparency");

78. Article 6(1) GDPR stipulates that the processing of personal data is lawful only if one of the conditions set out in Article 6(1)(a) to (f) is met. Compliance with Article 6(1) is referred to as having a "legal basis" for processing. Having a legal basis under Article 6(1) GDPR is necessary but not sufficient for processing to be lawful; controllers must also meet the broader obligations set out in the GDPR. Article 6(1)(e) GDPR states:

“Processing shall be lawful only if and to the extent that at least one of the following applies:

...(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”

79. Recital 42 provides:

“Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the ‘Court of Justice’) and the European Court of Human Rights.”

80. Recital 43 further provides:

“Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.”

81. Recital 45 provides:

“It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so”.

82. Article 9 relates to special categories of personal data. While Article 9(1) prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation, Article 9(2) disapplies this prohibition where, in relevant part:

“processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

[...]

processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;”

83. In this regard, Recital 52 provides:

“Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or

defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.”

iii. Clear, precise and foreseeable lawful basis

84. Limitations on rights must have a clear, precise and foreseeable basis in law on the basis of Article 6(3) GDPR and the case-law of the ECHR and CJEU, as outlined in more detail in this section.

Case-Law of the European Court of Human Rights

85. Article 8 of the European Convention of Human Rights provides:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

86. The European Court of Human Rights (“**ECtHR**”) has held that interferences with a person’s right to private life under Article 8(1) are only permissible, when such interferences are “*in accordance with the law*” and “*necessary in a democratic society.*”

87. One of the first cases to address the requirements of the phrase “*in accordance with the law*” under the Convention was *The Sunday Times v United Kingdom*.⁵⁴ The case concerned an alleged interference with the applicant’s right to freedom of expression under Article 10 of the Convention. The Court considered the meaning of the wording of Article 10(2) that any interference with the applicant’s right to freedom of expression should be “*prescribed by law*”:

“In the Court's opinion, the following are two of the requirements that flow from the expression “prescribed by law”. First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded

⁵⁴ (1979-80) 2 EHRR 245.

as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail...⁵⁵

88. Although, the words “*in accordance with the law*” as opposed to “*prescribed by law*” are used in Article 8(2), the Court held in *The Sunday Times* the expressions should be interpreted as similarly as possible.⁵⁶ Subsequent cases have given equivalent interpretations to the phrase “*in accordance with the law*” under Article 8(2).⁵⁷

89. *De Tommaso v Italy* recently summarised the case-law regarding the meaning of the phrase “*in accordance with the law*” under the Convention:

“The Court reiterates its settled case-law, according to which the expression “in accordance with law” not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the persons concerned and foreseeable as to its effects.”⁵⁸

90. A rationale for the interference being prescribed by legislation that is precise and foreseeable, is to ensure that the interferences with rights are not arbitrary.⁵⁹ If the legislation gives a broad discretion to an authority to allow interferences with a Convention right, it increases the likelihood the legislation has not been drafted with sufficient precision and that it does not provide protection against arbitrary interferences with rights.⁶⁰

91. The level of precision required in a legislative measure depends “on the content of the law in question, the field it is designed to cover and the number and status of those to

⁵⁵ Ibid at [49].

⁵⁶ Ibid at [48].

⁵⁷ See for example: *Huvig v France* (1990) 12 EHRR 528 at [26] and *Fernández Martínez v Spain* (App No 56030/07) at [117].

⁵⁸ *De Tommaso v Italy* (2017) 65 EHRR 19 at [106] citing *Khlyustov* (App No 28975/05) at [68], 11 July 2013; *X v Latvia* (2014) 59 EHRR. 3 at [58]; *Centro Europa 7 Srl v Italy* (App No 38433/09) at [140], 7 June 2012; *Rotaru v Romania* (App No 28341/95) at [52], 4 May 2000; and *Maestri v Italy* (2004) 39 EHRR 38 at [30].

⁵⁹ *S v United Kingdom* (2008) 48 EHRR 1169 at [99] and *Demirtas v Turkey* (2019) 69 EHRR 27 at [143].

⁶⁰ *Tommaso v Italy* (2017) 65 EHRR 19 at [118].

whom it is addressed.”⁶¹ It was noted in *S v United Kingdom* that the application of the law should:

*“be reasonably predictable, if necessary with the assistance of expert advice. But except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. It is enough that it lays down principles which are capable of being predictably applied to any situation.”*⁶²

92. Nonetheless, *Kopp v Switzerland* held that legal bases in respect of surveillance technologies should be “particularly precise”, considering their invasiveness and the fact technology increases in sophistication over time.⁶³ This principle is relevant when considering the use of facial matching technology used by the DSP. Such processing involves the creation of biometric data relating to the individual. This level of intrusion on the fundamental rights of the individual based on this use of technology and biometric processing requires particularly precise legal justification.

Case-Law of the Court of Justice of the European Union

93. CJEU jurisprudence has also considered the requirements of clarity, precision and foreseeability in relation to laws which authorise the processing of personal data by state or public authorities. These requirements can be said to flow from the Charter of Fundamental Rights of the EU (“CFR”). Article 7 protects the right to one’s “*private and family life, home and communications.*” Article 8 states:

- “1. Everyone has the right to the protection of personal data concerning him or her.*
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
- 3. Compliance with these rules shall be subject to control by an independent authority.”*

⁶¹ *De Tommaso v Italy* (2017) 65 EHRR 19 at [108]. See also *Peruzzo and Martens v Germany* (2013) 57 EHRR SE17 at [35].

⁶² *S v United Kingdom* (2008) 48 EHRR 1169 at [99].

⁶³ *Reports of Judgments and Decisions* 1998-Ithe DPC, 25 March 1998, § 55 at [72]. See also *Zakharov v Russia* (App No 47143/06) at [229]; *Centrum för Rättvisa v Sweden* (2019) 68 EHRR 2 at [101]; and *Big Brother Watch v United Kingdom* (App Nos 58170/13, 62322/14, 24960/15) (Grand Chamber) at [333].

94. The requirement that a legal basis permitting the processing of personal data be clear, precise and its application foreseeable, can in particular be said to derive from Article 52 of the Charter which states:

“1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.”

95. In C-362/14 *Schrems v Data Protection Commissioner* (*‘Schrems I’*) the CJEU invalidated the Safe Harbour Agreement, which had until that point, provided the legal framework for data transfers from the EU to the US. In the case the CJEU commented on the need for a law permitting interference with rights under Article 7 and 8 of the Charter to be clear and precise:

“EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court’s settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.”⁶⁴

96. In Case C-175/20 *SIA ‘SS’ v Valsts ieņēmumu dienests*, Advocate General Bobek indicated that if a legal basis lacks the requisite detail required by Article 8(2) of the CFR, an alternative means of clarifying the scope of the personal data to be processed is at an administrative level:

“In other words, the two regulatory layers, namely the legislative and the administrative, making up the eventual legal basis for the data processing, operate jointly. At least one of them must be sufficiently specific and tailored to a certain type or a certain amount of personal data requested. The more there is at the legislative, structural level for such data transfers, the less there needs to be in the individual administrative request. The legislative layer might even be so detailed and comprehensive that it will be completely self-contained and self-executing. By contrast, the more generic and vague the legislative level, the more detail, including

⁶⁴ Case C-362/14 *Schrems v Data Protection Commissioner* EU:C:2015:650 at [91].

a clear statement of purpose which will thus delimit the scope, there will need to be at the level of the individual administrative request.”⁶⁵

Conclusion on the requirement to have a clear, precise and foreseeable lawful basis

97. Recital 33 of the LED and Recital 41 GDPR emphasise the importance of the legal basis relied upon for the purposes of processing data being clear, precise and its application foreseeable in accordance with the case-law of the ECtHR and the CJEU. The DPC will therefore apply the case-law of those courts summarised above in assessing whether there is a valid legal basis for the processing of personal data under the GDPR.

iv. Necessity and proportionality

98. Necessity is an important concept in EU data protection law⁶⁶ with a specific meaning.⁶⁷ In several judgments, the CJEU has found that the processing of personal data, which is a limitation on the rights to privacy and personal data protection under Articles 7 and 8 of the CFR,⁶⁸ must be strictly necessary for the purposes pursued.⁶⁹ Thus, the European Data Protection Board (“**EDPB**”) has adopted guidelines stipulating that the strict necessity test precludes processing “which is useful but not objectively necessary.”⁷⁰ Relevantly, this strict necessity test has been applied to personal data processed for the establishment, exercise or defence of legal claims in the *Rīgas* judgment.⁷¹

⁶⁵ Case C 175/20 *SIA ‘SS’ v Valsts ieņēmumu dienests*, Opinion of Advocate General Bobek delivered 2 September 2021 at [82].

⁶⁶ For example, the European Data Protection Supervisor (“**EDPS**”) states that necessity “is an essential element with which any proposed measure that involves the processing of personal data must comply”. See “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit,” (11 April 2017) < <https://www.dataprotection.ie/sites/default/files/uploads/2022-09/02.09.22%20Decision%20IN%2009-09-22%20Instagram.pdf>>, page 2 (accessed 8 April 2025)

⁶⁷ Case C-524/06 *Huber v Bundesrepublik Deutschland*, Judgment of 16 December 2008 (“Huber”)

⁶⁸ EDPS, “The EDPS quick-guide to necessity and proportionality” (January 2020) < https://www.edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf> (accessed 8 April 2025).

⁶⁹ Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiksme’*, (“Rīgas”), Judgment of 4 May 2017, [30] (emphasis added).

⁷⁰ EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019 (“EDPB Guidance on Article 6(1)(b)”), p8.

⁷¹ *Rīgas* (op. cit.), [29] and [30].

Strict necessity has several elements. The interference with data protection must be capable of achieving its stated objective.⁷² CJEU case-law also underscores that processing of personal data is not necessary if there are “realistic, less intrusive alternatives.”⁷³ In that vein, there ought to be no equally effective available alternative manner of achieving the stated objective,⁷⁴ and any interference arising from the processing in question should be the least restrictive of the right.⁷⁵ The judgment of the Court in *V.S.*⁷⁶ is relevant in considering the elements for strict necessity. While this judgment concerned the LED, the assessment of strict necessity is equally applicable for the purposes of the GDPR. The Court held:

“Furthermore, the requirement that processing of sensitive data be ‘strictly necessary’ entails particularly strict checking, in that context, as to whether the principle of data minimisation is observed.

*In that regard, first, it must be borne in mind, as is apparent from recital 26 of Directive 2016/680, that the requirement of necessity is met where the objective pursued by the data processing at issue cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, paragraph 85 and the case-law cited). In particular, in the light of the enhanced protection of persons with regard to the processing of sensitive data, the controller in respect of that processing should satisfy itself that that objective cannot be met by having recourse to categories of data other than those listed in Article 10 of Directive 2016/680.*

Second, having regard to the significant risks posed by the processing of sensitive data to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the ‘strictly necessary’ requirement means that account is to be taken of the specific importance of the objective that such processing is intended to achieve. Such importance may be assessed, inter alia, on the basis of the very nature of the

⁷² Rigas (op. cit.), Opinion of Advocate General Bobek of 26 January 2017, [71].

⁷³ EDPB Guidance on Article 6(1)(b), [25], citing Rigas (op. cit.), [30] and Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, Judgment of 9 November 2010 (“Volker and Scheke”).

⁷⁴ Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, [88].

⁷⁵ In *Volker and Scheke* (op. cit) at [3], the CJEU held that it was “possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question...”.

⁷⁶ See *V.S. v Ministerstvo na vatreshnite raboti*, Glavna direksia za borba s organiziranata prestapnost, judgement of 26 January 2023, Case C-205/21, (ECLI:EU:C:2023:49).

objective pursued – in particular of the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats – and in the light of the specific circumstances in which that processing is carried out.

In view of the foregoing, it must be held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement laid down in Article 10 of Directive 2016/680 that processing of the special categories of data referred to in that article is to be allowed ‘only where strictly necessary’.

Such legislation is liable to lead, in an indiscriminate and generalised manner, to collection of the biometric and genetic data of most accused persons since the concept of ‘intentional criminal offence subject to public prosecution’ is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity.”⁷⁷

99. Proportionality is an assessment of the legitimacy of an aim, balanced against the scope, extent and intensity of the interference with a fundamental right.⁷⁸

100. The concept of proportionality is closely related to the necessity test.⁷⁹ In Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB*, the CJEU considered the interference with fundamental rights caused by a particular processing activity before applying the necessity test. Due to the “seriousness of the interference with fundamental rights” that arose from the relevant processing activity in that case the court found that only certain objectives pursued by processing could justify that interference.⁸⁰ In essence, the severity of interference with rights was balanced against the importance of the objective pursued by the processing in question, with the court stating:

“since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of

⁷⁷ Ibid at paragraphs 125 – 129.

⁷⁸ EDPS Guidelines on Proportionality (op. cit.), p10.

⁷⁹ EDPS Toolkit on Necessity (op. cit.), p5.

⁸⁰ Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis*, Judgment of 21 December 2016 (“Tele2 Sverige AB”), [102].

criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.”⁸¹

101. Therefore, in certain cases where interference with rights is sufficiently serious, it can be appropriate to consider the manner in which a particular processing activity interferes with fundamental rights in tandem with the necessity test. Generally, however, proportionality will be considered after the necessity test has been applied.⁸²

102. Whereas any processing of personal data amounts to an interference with the rights to personal data protection and private and family life under Articles 7 and 8 of the CFR,⁸³ the seriousness of that interference will depend on the context. The following factors are relevant to consider in that context:

- the scope of the processing, in terms of the number of people affected and whether it interferes with the privacy of persons other than the data subjects in question;
- the extent of processing, including the amount of information collected and the period over which the data were collected;
- the level of intrusiveness of the processing, taking into account the nature of the activity and whether it involves profiling or affects activities covered by duties of confidentiality;
- whether the processing concerns vulnerable persons; and
- whether it affects any other fundamental rights, such as the right to privacy.⁸⁴

v. Submissions of the DSP

103. As set out in paragraphs 52-59 of this Decision, while the DSP primarily maintains that the processing it is engaged in is for the purposes of the Part 5 of the 2018 Act, it also provides that, insofar as the GDPR applies, there is a sufficient lawful basis.

104. The DSP also made submissions on the lawfulness of processing in section 4 of its submissions on the Draft Decision.⁸⁵ Including:

- (i) The DSP submits that it has clear, precise and foreseeable legal basis in the relevant provisions of the 2005 Act and, insofar as there is any deficiency (which

⁸¹ Ibid, [115].

⁸² EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to the privacy and to the protection of personal data, 19 December 2019 (“EDPS Guidelines on Proportionality”), p10.

⁸³ EDPS Quick Guide (op. cit.).

⁸⁴ EDPS Guidelines on Proportionality (op. cit.), p23-24.

⁸⁵ Appendix D.10.1.

is not accepted by the DSP), that deficiency is remedied by the additional administrative material explaining the processing conducted. The DSP submits that the DPC's analysis of the lawful basis for the biometric processing is largely confined to a misconceived interpretation of the individual statutory provisions of the 2005 Act and effectively ignores other legitimate and recognised methods, including the "administrative" layer of information (which it separately acknowledges to be comprehensive), the text of the GDPR (but not the LED) and the text of the Data Protection Act 2018 itself, through which data subjects should be aware that their data may be so processed.

- (ii) The DSP further submits that the DPC relies on a on a flawed and partial analysis both of the legal framework within which the DSP processes personal data and the documentation and evidence provided by the DSP with respect to this processing. The DSP submits that this is particularly the case with respect to its consideration of the purpose for which the DSP conducts facial image matching as part of SAFE 2 registration, the foreseeability by data subjects of that processing and its legal basis, and in its assessment of necessity and proportionality
- (iii) The DSP further submits that in its analysis of the purpose of facial image matching, the DPC parses text of a short customer information leaflet issued by the DSP to determine that the primary purpose of the processing is to issue a PSC. The DSP states that this is to unfairly ignore or improperly interpret the much more detailed text of the DSP's Privacy Statement and the Comprehensive Guide to SAFE Registration and the PSC documents. The DPC has also misunderstood and misapplied the applicable law. The DSP also submits that in its assessment of the "clarity, precision and foreseeability" of the lawful basis, the DPC errs in finding that no method of identity authentication is specified in the 2005 Act and that there is no level of identity assurance set out in the Act, in circumstances where the only method of identity authentication specified in the Act is that accepted as being SAFE 2 registration. The DPC also errs by not properly considering the abundance of information with respect to SAFE 2 registration, including the biometric element of that process, in the administrative layer of publicly available documents and information.
- (iv) The DSP states that in its assessment of necessity, the DPC errs in testing the concept against what it perceives to be the benefit of the processing (which in any case it grossly undervalues) rather than against the requirements that processing is necessary for the *performance of the authority/specific right* granted to the Minister under legislation to take and retain a photograph in electronic form for the purpose of the authentication of the identity of the person at any time.

- (v) The DSP states that the DPC fails to apprehend that a comparison of photographic images at large scale, necessary to assure that identity is not claimed fraudulently, must of necessity be performed using electronic methods which are, in turn, dependent on the conversion of those images into a numeric template. Neither does the DPC identify any feasible alternative means by which the Minister could exercise their right to authenticate identity using electronic records of photographic images in the context of the very large client base it serves nor the very large volume of transactions it processes.
- (vi) Furthermore, the DSP submits that in its assessment of proportionality, the DPC grossly underestimates the utility and value, including the public interest value, of the processing, fails to properly assess the crime prevention value of the processing, does not acknowledge that the processing does not reveal any private and personal information not already known to the DSP and moreover does not identify any material or incremental harm to data subjects arising from this processing against which this utility and value should be weighed.
- (vii) The DSP then submits that as a consequence, the DPC's findings are seriously flawed. This is particularly the case concerning the conclusion that the purpose of biometric processing for facial image matching purposes is not primarily concerned with the prevention, detection, investigation and/or prosecution of offences and the conclusion that the biometric processing for facial image matching purposes does not have a lawful basis.
- (viii) Finally, the DSP submits that the DPC errs in finding that the DSP has acted negligently in conducting biometric processing for facial image matching purposes. The DSP submitted that, at all times it honestly and reasonably believed, and continues to believe, that the processing concerned is in compliance with the GDPR/LED, does include appropriate safeguards and is communicated transparently to data subjects.

vi. Analysis

105. As noted above, the DPC considers that Part 5 of the 2018 Act (giving effect to the LED) does not apply to the DSP's processing of biometric data in SAFE 2 registration.

106. As is clear from an examination of the relevant provisions of the GDPR, in order for the collection of biometric data in SAFE 2 registration to be lawful under Article 6(1)(e) GDPR, such processing should have a basis in Union or Member State law. To that end, it must be determined if such a legal basis is clear, precise and foreseeable. It must also be considered whether processing is necessary and proportionate for the relevant purposes.

107. Before going into a more detailed examination of those issues, it is necessary to note from the outset, that in its submissions, quoted in paragraph 56, the DSP asserts that in Part 3.2.7 of its Final Investigation Report, the DPC accepted that the provisions in section 263B correspond to the SAFE 2 registration requirements.⁸⁶ This is, with respect, not what was accepted. Rather, it was determined at [175]-[177]:

“[The DSP] processes personal data consisting of all of the elements of the PSI dataset which may in turn need to be proved by the items described above in relation to: (A) evidence of identity; (B) evidence of address; and (C) additional documents to confirm identity. The references in this report to the processing carried out by DEASP in relation to SAFE registration and the issuing of PSCs relate to this personal data, unless other or specific types of personal data are being referred to.

It is also important to note that a second report will consider processing of personal data which is not covered by the preceding paragraph, but which takes place in the context of SAFE 2. This will include processing operations, including processing of sensitive personal data (now known as special category personal data under the GDPR), and personal data consisting of arithmetic templates of photographs (i.e. the data used by DEASP to conduct processing by way of facial matching) amongst other things. As stated in Part 1, processing by DEASP involving facial matching in relation to SAFE registration and the issuing of PSCs will be the subject of a separate report by the DPC. That report may also address the processing of other personal data which falls outside the personal data described above at paragraph 175 to 176.”

108. While the DPC considered that section 263B corresponded to the specified categories of documents, it expressly did not consider whether the processing of biometric data fell within this section. To that end, to the extent to which this is asserted for the purposes of suggesting that the DPC has in any way already accepted that there is a sufficient legal basis for the processing of biometric data, that assertion is misconceived.

109. Turning to the question of lawful basis, it is necessary to examine each of the specific statutory provisions relied upon by the DSP, how they interact, and whether they provide a clear, precise and foreseeable legal basis for such processing. Subsequently, it will be considered whether the processing is necessary and

⁸⁶ Appendix D.10.1, p96.

proportionate, before considering the additional legal conditions applicable to special categories of personal data.

Clear, precise and foreseeable lawful basis

110. Above, the DPC determined that the GDPR applies to the processing of biometric data for the purposes of authenticating identity in the context of issuing a PSC. The relevant provisions of the 2005 Act relating to that purpose are sections 241, 242, 247C, 262, 263 and 263B. The DSP also sought to rely on sections 250 and 251 of the 2005 Act as lawful bases under the LED. Those provisions will be considered in this section in the interests of completeness.

111. Per section 241 of the 2005 Act, it shall be a condition for any person's right to any benefit that they satisfy the Minister as to their identity. It is relevant to note that the duty to satisfy the Minister as to identity is on the individual claimant under section 241 not the Minister as submitted by the DSP in their submissions to the Draft Decision.⁸⁷ Per section 241(1C), to do so, the Minister "may", without prejudice to any other method of authenticating the identity of that person, request that person attend an office of the Minister or other place, provide such information and to produce any document to the Minister as the Minister may reasonably require:

"to allow a photograph or other record of an image of that person to be taken, at that office or other designated place, in electronic form, for the purpose of the authentication, by the Minister, at that time, of the identity of that person"

Section 241(1C) affords the Minister the discretion with regard to how the Minister may be satisfied as to a person's identity.

112. Section 242(4) provides that a person presenting for payment of benefit shall satisfy the Minister, an officer of the Minister or a payment service provider, as to their identity by furnishing his or her PSC, or a card that has been issued to the person by the Minister under section 264 and such other information or documentation as the Minister, an officer of the Minister or a payment service provider, as the case may be, may reasonably require for the purposes of authenticating the identity of that person.

113. Section 247C provides that the Minister may give notice to any person receiving a benefit requesting the person to satisfy the Minister as to their identity. Such a notice "may", without prejudice to any other method of authenticating the identity of that person, request the person to attend an office of the Minister or other place, provide such information and to produce any document to the Minister as the Minister may

⁸⁷ Appendix D.10.1, at p625.

reasonably require, to allow a photograph or other record of an image of that person to be taken, and to provide a sample of their signature in electronic form for the purposes of the authentication of their identity. This authentication process is also discretionary. This provision also makes no reference to biometric processing.

114. Per section 262, the Minister may allocate and issue a PPSN to each person who is the subject of any transaction with a specified body. The Minister shall not allocate and issue a PPSN to a person unless the Minister is satisfied as to the identity of the person. For the purposes of allocating and issuing PPSN, a person shall give to the Minister the categories of information set out under section 262(3)(a).

115. Section 263 provides the Minister may issue a PSC to a person in such form as the Minister considers fit for the purposes of carrying out a transaction. The Minister shall not issue a PSC to a person unless the Minister is satisfied as to the identity of the person to whom such card is to be issued. Per section 263B, for the purposes of authenticating a person's identity, the Minister "may", without prejudice to any other method of authenticating the identity of that person, request that person attend an office of the Minister or other place, provide such information and produce any document to the Minister as the Minister may reasonably require, allow a photograph or other record of an image of that person to be taken, and provide a sample of their signature in electronic form for the purposes of the authentication of their identity. This authentication process is also discretionary and without prejudice to any other forms of identification. This provision also makes no reference to biometric processing.

116. While the Minister for Social Protection is required to be satisfied as to a person's identity as a pre-condition to the provision of a number of welfare benefits, it is not directly stated that the methods through which the Minister may so satisfy themselves include biometric processing. Certain of the provisions outlined above permit the taking of photographs or other "*records of an image (...) in electronic form*". "Record" is defined in section 2(1) of the 2005 Act as "*any book, document or any other written or printed material in any form including any information stored, maintained or preserved by means of any mechanical or electronic device, whether or not stored, maintained or preserved in a legible form.*" In turn, "electronic" is defined in section 2(1) of the 2005 Act as including biometric technology. However, it is not mandatory for the Minister to use biometric data to verify identity prior to the issuance of a PSC or any benefits; the manner in which the Minister does so is at the Minister's discretion.

117. The provisions do not specify a particular method, nor do they require that the Minister must be "substantially assured" as to a person's identity either through the processing of biometric data or otherwise. Insofar as Article 6(1)(e) is concerned, there appear to be no limits or parameters set for the exercise of this discretion at all. Neither does the Minister have an obligation to process biometric data or indeed to always process biometric data in order to verify identity. There is nothing in any of the statutory

provisions that makes provision for (i) the biometric processing of all applicants for the relevant services; or (ii) the degree to which the Minister must be satisfied as to a person's identity. There is thus no clear, precise and foreseeable lawful basis under which the DSP may conduct biometric processing for the purposes of identity authentication for all PSC applicants.

118. From an examination of the relevant legal provisions of the 2005 Act, it would seem that the circumstances in which the Minister may choose to exercise their discretion to use biometric processing to verify identity is not clear, precise or foreseeable. It is simply not possible to anticipate from the wording of the legislation that the processing of biometric data would be utilised to authenticate identity or that this is a precondition for doing so. Therefore, there is no clear, precise and foreseeable lawful basis for this processing under Article 6(1)(e).

119. The DSP in its submissions on the Draft Decision⁸⁸ rejects the DPC's forgoing analysis and states that it does not follow the DPC's reasoning in the Draft Decision. Furthermore the DSP states that biometric processing is an optional power, which the DSP submits is "*not optional in practical terms*". The DSP's submissions also argue that the statutory power to engage in biometric processing is clearly set out in the 2005 Act. Notwithstanding the DSP's submissions, the DPC is satisfied that it has provided a clear explanation of why the 2005 Act does not provide a sufficiently clear and precise legal basis for the DSP to process biometric data in the context of SAFE 2 registration. In particular, the legislation relied upon by the DSP cannot be said to govern such a wide scope of processing and the DSP has not identified sufficient rules and safeguards that govern the scope and application of such biometric processing. In those circumstances, the legislation relied upon by the DSP does not bring clarity to the scope of the discretion conferred on the Minister as set out above.

120. In relation to Part 5 of the 2018 Act, the DSP has identified sections 250 and 251 of the 2005 Act as the underlying lawful basis for processing in order "*to detect, investigate and prosecute fraudulent misrepresentation or concealment of facts material to its functions under the SWCA 2005*".⁸⁹ Although it has been found that Part 5 of the 2005 Act is not relevant to the DSP's processing, this section considers sections 250 and 251 of the 2005 Act in the interests of completeness.

121. Section 250 of the 2005 Act provides that the Minister may appoint authorised officers to be Social Welfare Inspectors ("**SWIs**"), and sets out the powers of those inspectors. Section 251 sets out a list of offences relating to obtaining welfare benefits including on the grounds of false or misleading statements. Both sections fall short in

⁸⁸ Appendix D.10.1, p25.

⁸⁹ Appendix D.2.2, p17.

meeting the requirements of clarity, precision and foreseeability as to the biometric processing of personal data.

122. Most importantly, it should be noted that there is no reference in either of those provisions to conducting biometric processing for fraud prevention purposes.

123. Looking more particularly at section 251, this section makes it a criminal offence for a person to knowingly make any representation or knowingly conceal any material fact for any purpose connected with the Act. The fact that it is a criminal offence to conceal material is a deterrent measure against welfare fraud in and of itself. That section of the 2005 Act does not, in itself, make any provision for the DSP to also take further steps to prevent the perpetration of offences.

124. By contrast, section 250 has more relevance to the DSP's biometric processing for law enforcement purposes, but still falls short of the requirements of clarity, precision and foreseeability with regard to biometric processing. That section provides for the creation of SWIs and outlines their powers. SWIs have broad powers under section 250(2) to:

“investigate and report to the Minister on any claim for or in respect of benefit and any question arising on or in relation to that benefit, or an application for, or the use of, a personal public service number in accordance with sections 262 to 271 and any question arising on or in relation to that application or use which may be referred to him or her by the Minister, and may, for the purpose of the investigation and report require... [persons]... to give to the social welfare inspector the information and to produce to him or her the documents, within the period that may be prescribed, as he or she may reasonably require.”

125. This provision of the 2005 Act appears to relate to the circumstances in which the DSP may refer results of SAFE 2 registration to the SIU for further processing in the case of a suspected offence. This provision sets out the powers of SWIs, which are used in connection with the prosecution of specific suspected offences, as outlined in the DSP's submissions of 17 September 2021, *“In general, cases where fraud is ultimately detected arise from investigations undertaken by the Department's Special Investigations Unit and Social Welfare Inspectors.”*⁹⁰ This can be contrasted with the routine scanning of PSC applicants using SAFE 2 registrations. Section 250 contains further sub-sections relating to rent supplements, the power to enter premises, the payment of employment contributions and certain other matters. None of those sections relate to general powers to inspect welfare claims, and therefore the DPC does not consider them to be relevant to the biometric processing in SAFE 2 registration.

⁹⁰ Appendix D.2.2, p79.

Having regard to the sub-sections of section 250, section 250(2) alone is therefore relevant to consider.

126. However, there is no reference to biometric processing in section 250(2). While SWIs may obtain “information” and “documents,” those words are not defined in the 2005 Act. The definition of “records” includes a reference to electronic devices and in turn, the definition of “electronic” is defined to include biometric technology, but the words “record” and “electronic” are not included in section 250(2) of the 2005 Act. Claims may be referred to SWIs by the Minister, but there is no reference to the Minister referring claims on the basis of biometric scanning. Therefore, the provision gives no powers to the DSP to process biometric data for the purposes of investigating welfare fraud arising from the issuance of a PSC. It is not otherwise foreseeable from the wording of the sub-section that the DSP would engage in biometric processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

127. ‘SS’ v Valsts ieņēmumu dienests makes clear that if the primary legislation permitting processing of personal data is generic and broad, clarity can be achieved if an administrative request is sufficiently specific. The sections of the 2005 Act relating to fraud prevention have no references to biometric processing in a broad or generalised way. Therefore, this is not a question of a lack of specificity at legislative level that can be clarified further in an administrative act. There is no lawful basis, either specific or broad, to conduct biometric processing for these purposes.

128. Accordingly, in the absence of a specific lawful basis to process biometric data on a mass scale for the purposes outlined by the DSP, the DSP accordingly has no clear, precise and foreseeable lawful basis to process biometric personal data under the GDPR in the manner that it does.

Necessity and proportionality

129. Necessity is a precondition of relying on Articles 6(1)(e) GDPR and section 71 of the 2018 Act. Proportionality is also a general precondition for any interferences with fundamental rights under Article 51 of the CFR.

130. The EDPB Guidelines on the Use of Facial Recognition Technology state:

“Processing of special categories of data, such as biometric data can only be regarded as “strictly necessary” (Art. 10 LED) if the interference to the protection of

personal data and its restrictions is limited to what is absolutely necessary, i.e. indispensable, and excluding any processing of a general or systematic nature.”⁹¹

131. In its submissions on the Draft Decision, the DSP detailed the benefits of the PSC,⁹² and stated that the DSP consider that the processing of biometric of anyone who obtains a PSC is a sufficiently important aim and is wholly justified in the circumstances.⁹³ The DSP also stated in its submissions on the Draft Decision⁹⁴ that the low level of identified fraud as part of SAFE 2 registration does not indicate that the processing is disproportionate. The DSP also submitted that the low levels of fraud detection are evidence of the deterrent effect of biometric processing to the attempt of fraud in the first place.

132. In *RL v Landeshauptstadt Wiesbaden*⁹⁵, the CJEU considered the proportionality of the obligation laid down in Article 3(5) of Regulation 2019/1157 to include a facial image and two complete fingerprints in the storage medium of identity cards issued by Member States. The Court held that the legitimacy and significance of the objectives of combating the production of false identity cards and identity theft were in no way called into question by the fact that the number of detected fraudulent identity cards were low. The Court held that the EU legislature was not required to wait for that number to increase in order to be able to adopt measures to prevent the risk of such cards being used. The Court also held that:

“The assessment of the seriousness of the interference caused by a limitation on the rights guaranteed in Articles 7 and 8 of the Charter entails account being taken of the nature of the personal data concerned, in particular whether those data may be sensitive, as well as of the nature and specific arrangements for the processing of the data, in particular the number of persons who have access to those data and the arrangements for access to them. Where appropriate, account must also be taken of the existence of measures intended to prevent those data being the subject of unlawful processing.”

133. The DPC also accepts that the low levels of fraud identified by the DSP does not *ipso facto* point to a lack of proportionality. The DPC accepts that identifying even low levels of fraud can have an important deterrent effect and result in important savings for the exchequer over time. However, having regard to the provisions of the 2005 Act relied upon by the DSP, and the extent of the processing undertaken by it, the DSP has

⁹¹ EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (16 May 2022) at 4.

⁹² Appendix D.10.1, p10-11.

⁹³ Appendix D.10.1, p33.

⁹⁴ Appendix D.10.1, p39-43.

⁹⁵ Case C-61/22, *RL v Landeshauptstadt Wiesbaden*, judgment of 21 March 2024 (ECLI:EU:C:2024:251).

failed to demonstrate that the processing of biometric data for SAFE 2 registration is a necessary or proportionate interference with the rights to privacy or data protection. As set out above, as by 15 September 2021, the DSP held photographs and biometric templates in respect of 3,465,745 data subjects whose identity had been “*substantially assured*” by way of SAFE 2 registration. In addition, the DSP held photographs and biometric templates in respect of 22,356 people who had begun SAFE 2 registration but did not complete it. The number of data subjects in respect of whom the DSP held photographs and biometric templates was 3,488,101 on 15 September 2021.⁹⁶ Of the 3,465,745 people who had completed SAFE 2 registration on 15 September 2021, 13,103 of these were under 18 and 3,452,642 were 18 or over. On 15 September 2021, a total of 3,625,597 photographs had been used to generate a biometric template. This included templates created in respect of SAFE 2 registrations, PSC renewals and those awaiting PPSNs.

134. The DSP’s processing in respect of SAFE 2 registrations places no upper limit on the number of natural persons in relation to whom their personal data should be subjected to biometric processing. As set out below, this processing includes the DSP’s retention of the biometric facial templates for the lifetime of each person plus ten years, which infringes Article 5(1)(e) GDPR. The DSP has submitted that in order to appropriately pursue its identified purposes, it must subject virtually every single applicant and re-applicant for a PSC to biometric processing. As a corollary of this, while the DSP states that the requirement to obtain SAFE 2 registration and therefore be subject to biometric processing is not mandatory, it is required in order to access the range of welfare services provided by the DSP and none of the submissions nor the actual practice of the DSP suggest that there is any discretion in the DSP’s approach to subjecting applicants and re-applicants to biometric processing. Having regard to the high justification required under EU law and jurisprudence required to demonstrate the proportionality of any interferences with fundamental rights under Article 51 of the CFR, and having regard to the provisions of the 2005 Act and the lack of clear, precise and foreseeable safeguards governing the nature and specific arrangements for the processing of the data, the DSP has failed to demonstrate that the collection of biometric data of anyone who obtains a PSC is required for a sufficiently important public aim to justify this mass processing of personal data. Therefore, the DPC finds that the DSP failed to demonstrate the proportionality of that processing.

135. Accordingly, on the basis of all of the above, the DPC finds that the DSP has not complied with Article 6(1)(e) GDPR in relation to its processing of biometric data in SAFE 2 registration.

⁹⁶ Appendix D.2.2, p9.

Special category data

136. In relation to Article 9, as set out above, the processing of biometric data for the purposes of uniquely identifying data subjects constitutes the processing of a special category of personal data and accordingly, for the purposes of the GDPR, it must also be determined if any of the exceptions to the prohibition of processing under Article 9(2) apply. The DSP has specifically relied upon Article 9(2)(b) and (g). In relation to Part 5 of the 2018 Act, processing of special category data is permitted where it is necessary for “the performance of a function conferred on a person by or under an enactment.”⁹⁷
137. In relation to Article 9(2)(b), this arises where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject. As set out above, while the 2005 Act provides a basis for authenticating identity, such a basis is discretionary and does not clarify the circumstances in which biometric processing takes place or the safeguards for the fundamental rights and interests of data subjects. Accordingly, for the same reasons as arose in relation to Article 6(1)(e), such processing is not authorised by Member State law. Additionally, it is not explained, at all, how such processing – the processing of biometric data in relation to virtually every single applicant – is necessary for this obligation. There are also no apparent safeguards within the legislation for the fundamental rights and interests of the data subject, and none have been identified by the DSP. Indeed, in circumstances where the legislation does not refer to biometric processing at all, it would be difficult for that to be the case. The DPC would however note that from examining the practical implementation of safeguards by the DSP, it has no reason to believe that the personal data has not been kept and maintained securely.
138. In relation to Article 9(2)(g), this arises where processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Similarly, the requirements of necessity and proportionality are not met in the same circumstances as set out above in relation to Article 9(2)(b) and again there appear to be no legislative safeguards present or identified. More fundamentally, the DSP has not demonstrated how the processing of biometric data in relation to every applicant is proportionate to the aim of authenticating their identities. No submissions as to proportionality have been made,

⁹⁷ 2018 Act, section 73(1)(b)(iv)(II).

nor was the conduct of such an assessment apparent from any of the materials provided, including the DPIA.

Lawful basis under other sections of the 2018 Act

139. In addition to the provisions of the 2005 Act, the DSP also provides that a number of provisions of the 2018 Act can be relied upon as the legislation underlying its reliance on Article 6(1)(e) GDPR – in particular sections 38, 41, 46, 47 and 49 of the 2018 Act, and also, therefore, a legal basis exists under section 45.

140. Per section 38, the processing of personal data shall be lawful to the extent that such processing is necessary and proportionate for the performance of a function of a controller conferred by or under an enactment or by the Constitution, the administration by or on behalf of a controller of any non-statutory scheme, programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment or by the Constitution. For the same reasons as set out above, it has not been established that such processing on such a scale is necessary or proportionate for the performance of the DSP identity authentication function and so this cannot avail the DSP.

141. Section 41 provides without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes of (a) preventing a threat to national security, defence or public security; (b) preventing, detecting, investigating or prosecuting criminal offences; or (c) set out in paragraph (a) or (b) of section 47 – that is, for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. Section 41(a) does not apply to the DSP's processing in this Inquiry as it does not claim to process personal data for the purposes of preventing a threat to national security, defence or public security. Section 41(b) would only apply in respect of any processing covered by the LED or Part 5 of the 2018 Act, as it permits processing for the purposes of preventing, detecting, investigating or prosecuting criminal offences. For the same reasons that the processing does not fall within the scope of the LED, section 41(b) also does not apply to the DSP's processing. Turning to section 41(c), as set out below in relation to section 47, reliance on that provision is misconceived and so does not arise. Accordingly, section 41 cannot be relied upon.

142. Per section 46, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of

special categories of personal data shall be lawful where the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law. As set out above, while the DSP may require attendance or the provision of categories of personal data for the authentication of identity, this is discretionary and does not oblige the processing of biometric data. As well as this, no suitable and specific measures have been provided in the 2005 Act to safeguard the fundamental rights and freedoms of data subjects.

143. Section 47 states the processing of special categories of personal data shall be lawful where the processing is necessary for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. Reliance on section 47 is misconceived in circumstances where it is not clear and indeed unexplained how the authentication of data subjects' identities relates to legal claims, proceedings or legal rights. In any event, any purported reliance on section 47 could only arise subsequent to the processing of biometric data in SAFE 2 registration.

144. Per section 49, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where the processing respects the essence of the right to data protection and is necessary and proportionate for the administration of justice, or the performance of a function conferred on a person by or under an enactment or by the Constitution. As previously set out, the processing at issue has not been demonstrated as either necessary or proportionate, for the reasons provided above.

145. Finally, section 45 provides that, subject to compliance with the Data Protection Regulation and any other relevant enactment or rule of law, the processing of special categories of personal data shall be lawful to the extent the processing is authorised by section 41 and sections 46 to 54, or otherwise authorised by Article 9. As the DPC has determined that the provisions of section 41, 46, 47 and 49 as well as Article 9 do not authorise the DSP to process special categories of personal data, it necessarily follows that section 45 is not engaged either.

146. On the basis of all of the foregoing, the DPC has determined that there is an insufficient legal basis for the processing of biometric data by the DSP in SAFE 2 registration pursuant to the GDPR.

vii. Finding 1

147. In circumstances where the DSP does not have an adequate legal basis under Article 6(1)(e) for the collection of biometric data in connection with SAFE 2 registration,

the DPC finds that the DSP has not complied with its obligations under Article 5(1)(a) and Article 6(1) GDPR.

148. In circumstances where the DSP does not meet the provisions of Article 9(2)(b) and (g) GDPR, the DPC finds that the DSP does not have an adequate legal basis for the processing of a special category of personal data – biometric data – and so the DSP has not complied with Article 9(1) GDPR.

F. ISSUE 2: ASSESSMENT OF MATTERS CONCERNING THE RETENTION OF PERSONAL DATA

149. The DPC has determined that the GDPR applies to processing of biometric data in SAFE 2 registration. Therefore, as set out in the Inquiry Issues Paper, the DPC must now determine whether the DSP complied with the obligation regarding retention in the processing of personal data consisting of the processing of the biometric facial templates by way of facial matching during SAFE 2 registration under the GDPR and under Part 5 of the 2018 Act.

150. Above, it was considered whether the collection of biometric data for the purposes of the GDPR or Part 5 of the 2018 Act was lawful. By contrast, this section of the Decision considers the lawfulness of the retention of that data following its initial collection. Save where otherwise specified, the analysis and findings in this section of the Decision are without prejudice to the analysis and findings in relation to Issue 1.

151. With regard to the GDPR, retention will be examined having regard to submissions made by the DSP and Article 5(1)(e) GDPR.

a) Overview of the Relevant Legal Provisions

152. Having regard to the DSP's submission that it retains photographs and biometric facial templates for the lifetime of each person plus ten years, the DPC will examine this retention policy against the provisions of the GDPR and Part 5 of the 2018 Act.

153. Article 5(1)(e) GDPR provides that personal data shall be

“kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed;”

154. Recital 39 GDPR provides that a data controller should take steps to ensure that personal data are retained for no longer than necessary through the establishment of retention time limits or periodic review.

viii. Submissions of the DSP

155. In its submissions, the DSP stated that biometric templates are processed *“solely by the Department for the purpose of identity authentication under the provisions of the*

*SWCA 2005, as set out in the answers to Question 6.1.*⁹⁸ The submissions also clarified that biometric templates are not stored on the PSC.⁹⁹

156. As of 17 September 2021, the DSP said that it held photographs and biometric templates in respect of 3,465,745 data subjects.

157. The DSP cited the need to prevent identity theft and fraud as set out in Recitals 75, 85 and 88 GDPR as their justification for retaining photographs and biometric facial templates for the lifetime of each person plus ten years. The retention period purportedly enables:

- i. The protection of a data subject's identity even when the person is no longer transacting business with the DSP.¹⁰⁰
- ii. Protection of data subject's identity after death.¹⁰¹
- iii. Validation of a person's identity should they need to re-engage with the DSP.¹⁰²

158. The DSP also cites the powers extended to the Minister of Social Protection by the 2005 Act, namely to store the PSI data set in electronic form as the DSP can be called upon at any time to verify the identity of any person to whom it has issued a PPSN.¹⁰³

159. The DSP has additionally stated its intention to carry out a Data Protection Impact Assessment ("**DPIA**") in relation to the processing of the biometric templates, which will include a review of retention periods.¹⁰⁴

160. The DSP submits that it has a lawful basis for the processing of biometric data under SAFE 2 registration and on the basis that the processing is lawful it must be accepted that the DSP has a legal basis for the retention of biometric data.

161. The DSP also states that the DPC has accepted under the 2021 Settlement Agreement that a retention policy of a person's lifetime plus ten years is justified in respect of the other PSI identity characteristics collected and processed as part of SAFE 2 registration and question why the retention of biometric data should not have a similar retention period.

162. The DSP also submits that the retention of biometric data is necessary for SAFE 2 registration and is necessary for the process to run effectively and not just for data storage.

⁹⁸ Appendix D.2.2, p6.

⁹⁹ Ibid, p6-7.

¹⁰⁰ Appendix D.3.2, p10.

¹⁰¹ Appendix D.3.2, p11.

¹⁰² Appendix D.3.2, p10.

¹⁰³ Appendix D.3.2, p9-11.

¹⁰⁴ Appendix D.3.2, p11.

163. The DSP submits that the retention period is necessary to enable data subjects to engage with the DSP and access public services over their lifetime and to prevent identity fraud after death.

ix. Analysis

164. The DPC has examined the DSP's reasons for the retention periods it has put in place for photographs and biometric facial templates. A retention period for the lifetime of a person plus ten years is, on the face of it, considerable.

165. While retention is a distinct processing operation to collection, which was dealt with in Issue 1, some of the purposes for which the DSP retain biometric data are similar to the purposes for collection. In particular, where the DSP retain biometric data to later verify identity, this is interlinked with the processing for the purposes of authenticating identity. The DSP also processes personal data each time a one to many check is carried out. In these circumstances the processing of personal data is not related to the person to whom the biometric data relates. The DSP also seeks to rely on its powers under the 2005 Act to carry out this processing. For the same reasons as set out above in relation to the collection of this data for the purposes of authenticating identity, the DPC finds that the retention of personal data for the same purposes is unlawful. The overlap between these findings will be taken into consideration in the imposition of corrective measures.

166. In its submissions, the DSP sets out why it believes the existing retention period is necessary for SAFE 2 registration.¹⁰⁵ In particular, the DSP has submitted that this retention is necessary in relation to the aim of protecting the identity of welfare recipients¹⁰⁶. However, this is a different processing purpose to those that were outlined by the DSP in relation to authenticating identity. The DSP in its submissions on the Draft Decision ¹⁰⁷ states that the DPC is incorrect to treat the protection of a data subject's identity as a different purpose to identity verification. The DSP states that protection of identity is a by-product of identity verification. It is important to note that purpose limitation is a core principle of the GDPR, which stipulates that personal data must be collected for specified, explicit and legitimate purposes. Furthermore, Recital 39 GDPR emphasises that the "*specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data*". The purpose of processing in the context of the GDPR is therefore a key factor which may determine the nature and extent of a controller's obligations. As such,

¹⁰⁵ Appendix D.10.1, p46-48.

¹⁰⁶ Appendix D.10.1, p45.

¹⁰⁷ Appendix D.10.1, p112.

it is essential to the proper enforcement of the GDPR that supervisory authorities are able to make reasonable and objective assessments of the purpose of processing, taking into account the relevant facts. The purpose of verifying an individual's identity to confirm that they are entitled to access certain public services, is a separate purpose to protecting an individual's identity. Therefore treating a distinct processing purpose simply as ancillary outcome or by-product of a different purpose fails to meet the requirements for purpose limitation.

167. Furthermore, the DSP has failed to demonstrate how the retention of biometric data actually achieves this purpose. In fact, in the majority of cases the DSP need to refer identity checks for human evaluation. Therefore, it cannot be considered necessary to process biometric data in order to protect the identity of data subjects. It is also unclear that it is proportionate to this aim to process the personal data of millions of data subjects in the State.

x. Finding 2

168. In line with the analysis set out in this section, DPC finds that the DSP's retention of biometric data for 10 years plus the lifetime of the data subject does not comply with Article 5(1)(e) GDPR.

G. ISSUE 3: ASSESSMENT OF MATTERS CONCERNING TRANSPARENCY

169. As set out in the Inquiry Issues Paper, the DPC must now determine whether the DSP complied with the obligation of transparency in the processing of personal data consisting of the processing of the biometric facial templates by way of facial matching during SAFE 2 registration under the GDPR having regard to submissions made by the DSP and:

- i. Article 5(1)(a) GDPR and its requirement that data shall be processed in a transparent manner;
- ii. Article 12 GDPR;
- iii. Article 13 GDPR;
- iv. Article 14 GDPR.

170. The DPC will have regard to the sources and quality of information provided to data subjects about the processing of their biometric personal data by means of the facial matching of biometric facial templates.

171. Having regard to the material scope of the Inquiry and the issues considered herein, this section will focus on whether the DSP provided information about the purposes and lawful bases for processing in the information that it provided to data

subjects as well as data retention. Therefore, the analysis will consider Articles 13(1)(c) and 13(2)(a) GDPR.

a) Overview of the Relevant Legal Provisions

172. The GDPR requires that personal data must be processed per Article 5(1)(a) GDPR “lawfully, fairly and in a transparent manner in relation to the data subject”. Specific GDPR provisions are contained in Articles 12(1) and 13 GDPR regarding the information to be provided to data subjects. Article 12(1) GDPR addresses the quality of information to be provided to data subjects, as follows:

“The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language...The information shall be provided in writing, or by other means, including, where appropriate, by electronic means”.

173. Article 13(1) GDPR provides as follows:

“Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing”.

174. Article 13(2) provides:

“In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period”.

175. The WP29 has published Transparency Guidelines, which were subsequently endorsed by the EDPB in May 2018.¹⁰⁸

¹⁰⁸ Article 29 Data Protection Working Party, “Guidelines on transparency under Regulation 2016/679”, WP 260 rev.01 (Revised 11 April 2018).

176. The DPC previously considered the requirements of Article 13(2)(c) in its decision in Inquiry IN-18-12-2 into WhatsApp. In that decision, the DPC noted that the information should be provided in such a way that there is a clear link from:

“a. a specified category/specified categories of personal data, to

b. the purpose(s) of the specified processing operation/set of operations, and to

c. the legal basis being relied upon to support that processing operation/set of operations.”

xi. Submissions of the DSP

177. In their submissions, the DSP outlined their processes employed to observe transparency:¹⁰⁹

i. When attending a SAFE registration interview:

- A form which the applicant completes, also contains a Data Protection Statement which states:

“Customers are required to provide personal data to determine eligibility for relevant payments and benefits. Personal data may be exchanged with other government departments and agencies where provided for by law.”¹¹⁰

- Trained officers are available on site to answer questions about the process.
- A leaflet entitled *“SAFE Registration and your personal data”* is issued to applicants. This leaflet outlines the purposes and means of the data processing.

ii. The DSP Privacy Statement is viewable on the DSP website on gov.ie. Links to the site are also provided in the application form and SAFE registration leaflet mentioned above. Information is *“provided in a multi layered manner, where the most important points are highlighted, and data subjects are given further information where required.”¹¹¹* Section 12.4 provides information about biometric data processing. Data subject’s rights are covered in sections 13 and 14. The Privacy Statement was updated in 2019 in accordance with recommendations

¹⁰⁹ Appendix D.2.2, p32-33 and Appendix D.10.1 p49-56.

¹¹⁰ Appendix D.2.2, p39.

¹¹¹ Appendix D.2.2, p33.

by the DPC. Further updates were carried out in August 2022. Section 6 deals with the legal basis for processing. In relation to biometric processing, this section says:

“To the extent that the department processes special categories of personal data including biometric data and data concerning a person’s health, the legal bases upon which the department mainly relies are

Article 9 (2) (b) : processing is necessary for the carrying out of obligations and specific rights in the field of employment and social security and social protection law;

Article 9 (2) (g) : processing is necessary for reasons of substantial public interest

Article 9 (2) (h) : processing is necessary for the assessment of working capacity and the provision and management of social care systems and services.

6.2 The department operates under a number of Acts which provide that personal data may be legally processed. The main Act is the Social Welfare Consolidation Act 2005 (running consolidation), as amended. An administrative consolidation of the 2005 Act can be viewed here. There are also a number of other pieces of primary and secondary legislation that allow the department to process personal data. Should you wish to know more about these, please see the list which is included in Appendix 1.”

- iii. In 2017, the DSP also published its Comprehensive Guide to SAFE Registration and the Public Services Card which contains information on SAFE Registration, Public Service Identity and PSCs.¹¹² A webpage titled “Data Protection in the Department of Social Protection” is also linked on the DSP website to inform data subjects on how to exercise their rights under the GDPR.
- iv. The DSP indicated that its Comprehensive Guide to SAFE Registration and the Public Services Card contains information on SAFE Registration, Public Service Identity and PSCs.¹¹³ Specifically in relation to biometric processing the DSP stated:

“Questions 42 and 43 of the Guide, set out below, contain information relating to the biometric processing that occurs as a result of the facial matching process:

¹¹² Appendix D.5.1.

¹¹³ Appendix D.5.1.

Q.42 DOES THE PUBLIC SERVICES CARD STORE BIOMETRICS?

No. While the card does store a person's photograph it does not store the biometric or arithmetic template of that photograph. Nor is the biometric or arithmetic template of the photo stored in the PSI dataset or shared with other public bodies.

Q. 43 WHERE IS THE BIOMETRIC OR ARITHMETIC TEMPLATE OF THE PHOTOGRAPH STORED AND WHO HAS ACCESS TO IT?

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 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.”¹¹⁴

The Guide, which dates from 2017, is available on the DSP website.¹¹⁵

- v. In relation to retention of data, the DSP publishes a data retention policy on their website. However neither the Guide nor the Privacy Statement make any direct or specific reference to retention periods for biometric data. Section 11.1 of the Privacy Statement says:

“11.1 Social insurance contribution records, PPSN, past claim data and identity data are retained for the lifetime of the person concerned plus a period of ten years. This is required for a number of reasons:

First, in order that a person can claim entitlement to services and benefits – many of which may not fall due until the occurrence of a particular event during the lifetime of a person – the date of which cannot be known, for example illness, disability, caring responsibilities or widowhood.

Second, PPSN and identity data is critical to the prevention, detection and prosecution of identity fraud, which again can occur at an unknown time. It is also critical to the efficient administration of estate cases (i.e. payments made or refunded after a person dies). Estate cases can take a number of years to resolve.

Third, prior claim data is required because it can affect entitlement to future payments, because, under law, a person can request a review in respect of any claim decision at any time. Also it can be necessary to inform an investigation into a prior fraud or error which is detected on the occasion of a subsequent claim or life event.”

178. With regard to the applicability of Article 14 GDPR, the DSP states that this applies where data is not obtained from the data subject, which is not the case in the instant inquiry.¹¹⁶

¹¹⁴ Appendix D.2.2, p34-35.

¹¹⁵ Department of Employment Affairs and Social Protection, ““COMPREHENSIVE GUIDE TO SAFE REGISTRATION AND THE PUBLIC SERVICES CARD” (October 2017), < <https://www.gov.ie/pdf/?file=https://assets.gov.ie/70988/151dd4b4cbe249439af72fa7c76fa874.pdf#page=null>> (accessed 7 April 2025)

¹¹⁶ Appendix D.7.1, p12.

xii. Analysis

179. Having carefully examined all of the information provided by the DSP with regard to its transparency obligations in relation to the processing of biometric facial templates, the DPC considers that the information provided by the DSP in the course of SAFE 2 Registration and online to individuals in relation to the purposes of processing biometric data to be comprehensive in nature. However, the information is not displayed in a manner that draws a clear link from the categories of personal data to the purposes to the lawful bases. The purposes and lawful bases are set out in different sections of the Privacy Policy, appearing in sections 6 and 12 respectively, with no clarity as to the specific lawful basis for biometric processing. The Privacy Statement uses vague catch-all language regarding three different lawful bases without specificity as to its actual lawful basis for processing. The DPC therefore considers that the DSP has infringed Article 13(1)(c) GDPR in relation to the transparency of its processing of biometric facial templates as part of SAFE 2 Registration. This is without prejudice to the findings above regarding the lack of a lawful basis for this processing.

180. In relation to Article 13(2)(a) GDPR, as noted above, the DSP has a data retention policy which is accessible from the DSP's Privacy Statement. However, the Privacy Statement does not make any direct reference to the length of time for storing biometric data. The Privacy Statement separately refers to biometric processing, but in the section on data retention there is no reference to biometric storage. There is therefore no clear indication in that statement that biometric data are stored for the data subject's lifetime plus ten years.

181. Similarly, the DSP's retention policy does not expressly state that biometric data collected during SAFE 2 registration is retained for the lifetime of the data subject plus ten years. The retention policy states as follows at paragraph 10.1:

"Social insurance contribution records, PPSN, past claim data and identity data are retained for the lifetime of the person concerned plus 10 years."

182. The retention policy separately defines the term special category data at paragraph 4 of the retention policy to include biometric data, however there is no reference to biometric data at paragraph 10.1 of the retention policy which sets out the retention periods. The retention periods for biometric data are not sufficiently clear in the retention policy.

183. The DPC therefore finds that the DSP has infringed Article 13(2)(a) GDPR.

xiii. Finding 3

184. In relation to its GDPR purpose of authenticating identity, the various sources of information provided by the DSP infringed Articles 13(1)(c) and 13(2)(a) GDPR.

H. ISSUE 4: ASSESSMENT OF MATTERS CONCERNING THE REQUIREMENT TO HAVE UNDERTAKEN A DATA PROTECTION IMPACT ASSESSMENT

185. As set out in the Inquiry Issues Paper, the DPC must now determine whether the DSP complied with the requirement to have undertaken a DPIA with regard to the processing of personal data consisting of the processing of the biometric facial templates by way of facial matching during SAFE 2 registration under the GDPR and under Part 5 of the 2018 Act.

186. With regard to the GDPR, this will be examined having regard to Article 35 GDPR.

a) Overview of the Relevant Legal Provisions

187. Article 35 GDPR sets out the requirement to conduct a DPIA in certain circumstances. It states in paragraphs (1) and (3):

“1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

[...]

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

c. a systematic monitoring of a publicly accessible area on a large scale.”

188. Supervisory authorities such as the DPC are required to publish a list of the “*kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.*”¹¹⁷

189. Under Article 35(7) GDPR, the assessment shall contain at least:

“a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.”

190. Recital 90 further provides:

“In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.”

191. And Recital 91:

“This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where

¹¹⁷ GDPR, Article 35(4).

those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.”

192. The Article 29 Working Party has also prepared Guidelines on Data Protection Impact Assessments.¹¹⁸ It states at 6:

“In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

193. Additionally at 9-10, it states:

“In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under

¹¹⁸ Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (4 October 2017) WP 248 rev.01.

article 35(4) and recitals 71, 75 and 91, and other GDPR references to “likely to result in a high risk” processing operations , the following nine criteria should be considered.

[...]

4. *Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients’ medical records or a private investigator keeping offenders’ details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.*

5. *Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.*

6. *Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject .*

[...]

8. *Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in “accordance with the achieved state of technological knowledge” (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain “Internet of Things” applications could have a significant impact on individuals’ daily lives and privacy; and therefore require a DPIA.*

9. *When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.”*

194. The Guidelines additionally state at 13-14 that:

“The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

[...]

As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.”

195. The DPC itself also has a Guidance Note on DPIAs.¹¹⁹ This states at 4-5:

“In addition to the general conditions outlining when a DPIA is necessary, the DPC adopted the following list, pursuant to Article 35(4) GDPR, specifying certain types of processing for which a DPIA is mandatory: 1) Use of personal data on a large-

¹¹⁹ Data Protection Commission, “Guide to Data Protection Impact Assessments” (October 2019), <https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf> (accessed 7 April 2025)

scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4). 2) Profiling vulnerable persons including children to target marketing or online services at such persons. 3) Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects. 4) Systematically monitoring, tracking or observing individuals' location or behaviour. 5) Profiling individuals on a large-scale. 6) Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines. 7) Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines. 8) Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort. 9) Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for different purposes or by different controllers. 10) Large scale processing of personal data where the Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals."

196. It further states at 10-11:

"The GDPR became effective from the 25 May 2018, and the Article 29 Working Party/EDPB guidelines specifically noted that the requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing."

xiv. Submissions of the DSP

197. In its submissions, the DSP stated that it did not carry out a DPIA in relation to its processing of biometric data at the time of the coming into force of the GDPR, but did carry one out at the time of an upgrade to the facial image matching system. The first version of the DPIA was produced in February 2020. In its submissions, the DSP stated that:

“In May 2018, there was no change to the risks involved in the processing of biometric data by the Department since its introduction in 2013.”¹²⁰

198. In 2018, the DSP engaged in a procurement process for the supply, configuration and integration of facial matching software in connection with SAFE 2 registration, to replace or upgrade the facial matching software previously procured in 2012.

199. With regard to the upgrade, the DSP stated¹²¹ that:

“In common with other organisations and as part of its standard processes, the Department from time to time upgrades its software applications to ensure that it is operating using the latest version/generation of software available. This is necessary to ensure that the Department has access to support and maintenance from software vendors, to take advantage of any performance or functionality improvements in newer generation software and to assure inter-operability of software applications with underlying technical hardware and operating systems.

The facial matching system was over 5 years old at the time of the new tender process in 2018.

The procurement undertaken in 2018 was required to assure the continued performance and functionality of the facial image matching software and was timely given the Department was introducing a process whereby existing PSC holders could renew their PSCs as they expired, i.e. to introduce a ‘one-to-one’ facial image matching process. The procurement process was carried out via eTenders and the Request for Tender (RFT) document was publicly available. The upgrade went live on 27th January 2021. From that date, a one-to-one match is first carried out in respect of each PSC renewal, before the one-to-many match is carried out.”

200. The DPIA carried out in relation to the upgrade identified 12 potential risks with regard to the following data protection principles:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality

¹²⁰ Appendix D.3.2, p6 and Appendix D.10.1, p59.

¹²¹ Appendix D.2.2, p21-22.

- Accountability

201. Each risk was assigned proposed actions. In the DPIA, the DSP stated:

“Of the 12 potential risks identified, all risks have been mitigated with the proposed 20 actions...”¹²²

[...]

The Department has undertaken a review of the high risks associated with the upgraded Facial Matching Software. The risks identified are being mitigated through several actions as outlined... The Department is dedicated to completing the actions identified to mitigate the risks identified.

On an ongoing basis, the Department will review and update the adequacy of the risks identified and actions agreed in the DPIA.”¹²³

202. The DSP stated that it is committed to carrying out a further DPIA with regard to its processing of biometric data. In its submissions, the DSP stated

“The Department is happy to commit to carrying out a DPIA on the processing of biometric data in relation to SAFE registration and looks forward to working with the Commission on this project.”

203. In its submission on the Draft Decision¹²⁴ the DSP states that Article 35 GDPR did not require a DPIA for pre-existing processing operations upon the GDPR’s entry into force. The DSP submits that the Article 29 Working Party Guidelines specify two cumulative conditions for requiring a DPIA for such processing operations:

- (i) a likelihood of high risk to the rights and freedoms of natural persons, and
- (ii) for which there has been a change of risks since prior assessments under Directive 95/46/EC.

The DSP asserts that the conditions of its biometric data processing, established in 2012, remained consistent, with no alteration in scope, purpose, or implementation that would constitute a change in risks. Consequently, the DSP submits the second criterion was not satisfied, negating any obligation to conduct a DPIA in 2018.

¹²² Appendix D.2.3, p10.

¹²³ Appendix D.2.3, p22.

¹²⁴ Appendix D.10.1, p57-62.

204. With regard to Article 35(7)(b) GDPR, the DSP maintains in its submissions on the Draft Decision that the DPIA did include an evaluation of the necessity and proportionality of the processing operations directly associated with the software upgrade. The DSP states that the DPIA at section 4.3.1 includes the legal basis for the processing as required by Article 35(7)(c) GDPR. The DSP submits that this inclusion of the legal basis in the DPIA evidences the DSP's continued satisfaction with this legal basis.

xv. Analysis

205. Given the scale of processing involved, given that the processing involves high risks on that basis and that it relates to a special category of personal data, and given that it involves both by its very scale and the purpose of the processing – that is, access to benefits provided by the DSP – the processing of the personal data of vulnerable data subjects – which include pregnant people, persons with disabilities and the elderly – the DPC finds that the DSP was under an obligation to conduct a DPIA at the time of an upgrade to the facial image matching system. The processing involves special categories of personal data and took place on a large scale, as it involves the processing of biometric data of anyone who sought to access a PSC. The processing could have resulted in the denial of access to certain public services, which is also relevant for consideration under the Article 29 Working Party Guidelines.

206. The DPC finds that the DPIA carried out by the DSP does not meet all of the requirements of Article 35(7) GDPR. The DPIA does contain a detailed analysis of the processing and risk mitigating measures and therefore, the DPC does not find an infringement of Articles 35(7)(a) or 35(7)(d). However, the DPIA does not include any details of why the processing is necessary or proportionate for the purposes pursued. On that basis, the DPC finds an infringement of Article 35(7)(b) GDPR. The DPIA also does not identify a possible risk being the lack of a lawful basis for processing. It states that there is a risk of re-use without a lawful basis. It also briefly summarises the provisions of the 2005 Act upon which the DSP seeks to base the processing. However, it does not engage in any detailed analysis of whether those legal provisions provide a lawful basis for the processing at issue. It therefore does not identify a relevant risk associated with this processing activity. This amounts to an infringement of Article 35(7)(c) GDPR.

xvi. Finding 4

207. In light of the risks of varying likelihood and severity for the rights and freedoms of natural persons, in particular the inherently sensitive nature of that personal data and the large scale of the data processing, the DSP has infringed Articles 35(7)(b) and

(c) GDPR by failing to include certain details in the DPIA that was carried out in February 2020.

I. FINDINGS

208. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, findings that the DSP has infringed the following Articles of the GDPR:

- a. Article 5(1)(a), Article 6(1) and 9(1) GDPR;
- b. Article 5(1)(e) GDPR;
- c. Article 13(1)(c) and 13(2)(a) GDPR; and
- d. Article 35(7)(b) and (c) GDPR.

209. Under section 111(2) of the 2018 Act, where the DPC makes a decision, it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) with respect to the GDPR and, if so, which corrective powers.

210. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor under the GDPR. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

“...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...”

211. The DSP made submissions on the corrective powers proposed by the DPC in the Draft Decision, in particular in relation to the proposed order to cease processing.¹²⁵ The DPC have taken into account the DSP’s submissions in relation to this order and in particular have considered the stated impact on data subjects and the State’s social protection infrastructure set out in section 8 of the DSP’s submissions on the Draft Decision. The DPC has adjusted this order as set out below.

212. The DPC has taken into account the DSP’s submissions on the timeline for compliance, as set out in paragraph 203 of the Draft Decision and as adjusted the order in the terms set out below.

¹²⁵ Appendix D.10.1, p63-79.

213. Having carefully considered the infringements identified in this Decision, and the submissions by the DSP in relation to the Draft Decision, the DPC has decided to exercise certain corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR. In summary, the corrective powers that the DPC has decided are appropriate to address the infringements in the particular circumstances are:

- a. An order pursuant to Article 58(2)(f) to the DSP to cease the processing of biometric data with regard to SAFE 2 registration;
- b. A reprimand to the DSP pursuant to Article 58(2)(b) GDPR; and
- c. Administrative fines for breaches of the GDPR.

214. Further detail is set out below in respect of each of these corrective powers that the DPC will exercise and the reasons why the DPC has decided to exercise them.

J. ORDER TO CEASE PROCESSING.

215. Article 58(2)(f) GDPR provides that a supervisory authority shall have the power:

“...to impose a temporary or definitive limitation including a ban on processing;”

216. In circumstances where the DPC has found that the processing at issue is not in compliance with the GDPR, the DPC proposes making an order pursuant to Article 58(2)(f) GDPR. In particular, the DPC proposes ordering the DSP to cease the relevant processing given that it does not have a legal basis. The order under Article 58(2)(f) applies to the extent that the DSP is conducting ongoing processing operations as described in this Decision. Specifically, to the extent that the DSP is engaged in the processing of biometric data without a legal basis as described, this order requires the DSP to cease such processing within 9 months of this Decision if the DSP does not identify a valid lawful basis.

217. For the avoidance of doubt, the order refers to ‘processing’ as defined in Article 4(2) GDPR, to include collection, recording, storage and use of biometric data.

218. The order is made to ensure that full effect is given to the DSP’s obligations under these articles. The DPC considers that this order is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

219. The DPC considers that this order is necessary to ensure that full effect is given to the DSP obligations in relation to the infringements outlined above. The substance of this order is the only way in which the defects pointed out in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that the DPC finds that this power should be imposed.

220. Such an order is proportionate and is the minimum order required in order to guarantee that compliance will take place in the future. On that basis, the DPC is satisfied that the order is a necessary and proportionate action.
221. The order applies only insofar as is necessary for the DSP to cease processing that is not in compliance with the above stated provisions of the GDPR. Plainly, in order to do so, the processing outlined in this Decision, to the extent that it continues to fail to be in compliance with the provisions of the GDPR, must cease.
222. This order should be complied with within 9 months of the date of notification of this decision, given the significant financial, technological and human resources at the DSP's disposal. The DPC therefore requires the DSP to comply with the above order within 9 months of the date of notification of the final decision. Further to this, the DPC requires the DSP to submit a report to the DPC within that period detailing the actions it has taken to comply with the order.

K. REPRIMAND

223. Article 58(2)(b) GDPR provides that a supervisory authority shall have the power:

“to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation”

224. The DPC has decided to impose a reprimand on the DSP for the infringements identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. Each of the infringements concern the personal data of a significant number of data subjects and relate to a special category of personal data and are serious in nature. A reprimand is appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance.
225. The reprimand is necessary and proportionate in addition to the order in this Decision. While the order would require specific remedial action on the part of the DSP, the reprimand formally recognises the serious nature of these infringements. The DPC considers that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by the DSP and other controllers or processors carrying out similar processing operations, in particular in respect of the processing of special categories of personal data. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that the DSP and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations.

L. DECISION ON ADMINISTRATIVE FINES

226. Article 58(2)(i) GDPR provides that a supervisory authority shall have the power:

“to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.”

227. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.¹²⁶ Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

228. As the DPC has identified infringements of the GDPR above, the DPC will decide whether to propose administrative fines in respect of those infringements. In conducting this assessment, the DPC has had regard to Article 83 GDPR, which sets out “General conditions for imposing administrative fines.” The DPC has also had regard to EDPB guidelines which are designed to ensure a harmonised approach to fining. These sets of guidelines include the EDPB’s Guidelines on the calculation of administrative fines (the EDPB Fining Guidelines),¹²⁷ and the Article 29 Working Party’s Guidelines on the application and setting of administrative fines (the A29WP Fining Guidelines),¹²⁸ which have been endorsed by the EDPB.

229. As a first step, the DPC will consider whether to impose a fine by applying the criteria set out in Article 83(2) GDPR. If the outcome of the assessment is that a fine should be imposed, then the DPC will proceed to calculate the amount, by reference to the criteria in Article 83(2) GDPR and by considering the other factors set out in Articles 83(1)-(9) that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles will inform the calculation of any fine that is imposed in this Decision.

a) Whether to impose an administrative fine

230. Article 83(2) GDPR states,

“Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and

¹²⁶ GDPR, rec 148.

¹²⁷ Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 2.1, adopted on 24 May 2023.

¹²⁸ WP253.

deciding on the amount of the administrative fine in each individual case due regard shall be given to the following...”

231. Article 83(2) goes on to list 11 criteria from (a) to (k) to be taken into account when deciding whether to impose an administrative fine. Those provisions are set out below where they are also applied to the infringements identified herein.

- i. **Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them**

232. Article 83(2)(a) requires consideration of the identified criterion by reference to “the infringement” as well as “the processing concerned.” The phrase “**the processing concerned**” in this Article 83(2) analysis should be understood as meaning all of the processing operations that the DSP carries out on biometric personal data in the context of SAFE 2 registration.

233. Considering next the meaning of “infringement”, it is clear from Articles 83(3)-(5), that “infringement” means an infringement of a provision of the GDPR. Above, the DSP was found to have infringed Articles 5(1)(a), 5(1)(e), 6(1), 9(1), 13(1)(c), 13(2)(a), 35(7)(b) and 35(7)(c) GDPR. Thus, “**the infringement**”, for the purpose of the DPC’s assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Articles 5(1)(a), 5(1)(e), 6(1), 9(1), 13(1)(c), 13(2)(a), 35(7)(b) or 35(7)(c) GDPR. While each is an individual “infringement” of the relevant provision, they all concern the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term “**infringements**” unless otherwise indicated.

234. As all of the infringements relate to the processing concerned, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) criteria in the context of the infringements generally.

Taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

235. This section will consider the nature scope or purpose of the processing concerned, before considering the number of data subjects affected and the level of damage suffered by them.

236. The **nature** of the processing can include:

“the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.”¹²⁹

237. Circumstances that can lead to supervisory authorities attributing more weight to this factor include:

“where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, where there is a clear imbalance between the controller and data subjects or where the processing involves children or other vulnerable data subjects.”¹³⁰

238. The nature of the processing relating to the infringements identified herein is the processing of biometric data to verify identity in the context of SAFE 2 registration. As a result of that processing, a decision is taken regarding whether a data subject will be issued with a PSC. This processing could have consequences for data subjects, as they may be unable to receive welfare payments if they are not provided with a PSC. The personal data at issue also related to a vulnerable cohort of data subjects – those accessing benefits provided by law by the DSP including pregnant persons, the elderly and persons with disabilities. Of the 3,465,745 people who have undergone SAFE 2 registration, 13,103 of these are under 18 and 3,452,642 are 18 or over. Therefore, some personal data of children are affected by the processing.

239. The **scope** of the processing is assessed:

“with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller... The larger

¹²⁹ EDPB Fining Guidelines [53.b.i].

¹³⁰ Ibid.

the scope of the processing, the more weight the supervisory authority may attribute to this factor.”¹³¹

240. In its Comprehensive Guide to the PSC, the DSP states:

“[A]ll recipients of welfare services and payments in Ireland have or will be asked to complete the SAFE registration process (some exceptions may be made for example in respect of people with profound disabilities). Failure to complete a SAFE registration process when requested can result in refusal of a new welfare claim or withdrawal of an existing payment or benefit.

The Department of Employment Affairs and Social Protection makes it clear to customers in receipt of welfare payments or entitlements that they do need to register to SAFE 2, in accordance with the relevant legislative provisions, to access or to continue to access those payments/entitlements.” (emphasis added)¹³²

241. The number of times the facial matching process was carried out in each year from 2018 to 2021 was:

- a. 403,567 (2018)
- b. 310,305 (2019)
- c. 170,595 (2020)
- d. 107,609 (January to September 2021)

242. This brings the total number of times the facial matching process was carried out to 992,076 (from Jan 18 to Sept 21).¹³³

243. Therefore, the scope of processing is broad. The text from the Comprehensive Guide quoted above says that all recipients of welfare services and payments in the State are subjected to SAFE 2 registration. The facial matching process was carried out 992,076 times over a period of 3 years and 9 months.

244. The EDPB fining guidelines state that the **purpose** of the processing:

“will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls

¹³¹ EDPB Fining Guidelines [53.b.ii].

¹³² Appendix D.5.1, p10.

¹³³ Appendix D.2.2, p11.

*within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity)."*¹³⁴

245. The purpose for which the DSP carries out the processing relating to the infringements identified herein is to verify identity for the purposes of issuing a PSC. As noted above, obtaining a PSC is a mandatory pre-requisite to obtaining certain welfare payments.

246. In relation to the **number of data subjects**, the EDPB Fining Guidelines state,

*"The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on "systemic" connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature."*¹³⁵

247. As of 15 September 2021, the DSP holds photographs and biometric templates in respect of 3,465,745 data subjects whose identity has been "*substantially assured*" by way of SAFE 2 registration. In addition, the DSP holds photographs and biometric templates in respect of 22,356 people who began SAFE 2 registration but did not yet complete it. The total overall number of data subjects in respect of whom the DSP holds photographs and biometric templates is 3,488,101.¹³⁶ As of 15 September 2021, a total of 3,625,597 photographs have been used to generate a biometric template. This includes templates created in respect of SAFE 2 registrations, PSC renewals and those awaiting PPSNs. This is a high number. The population of the State in 2021 was

¹³⁴ EDPB Fining Guidelines [53.b.iii].

¹³⁵ EDPB Fining Guidelines [53.b.iv].

¹³⁶ Appendix D.2.2, p9.

5,011,500.¹³⁷ Therefore, as of 2021, the DSP held biometric templates relating to 70% of the population of the State.¹³⁸

248. The **level of damage** is considered by reference to any harm suffered by data subjects or the “extent to which the conduct may affect individual rights and freedoms.” The EDPB Fining Guidelines note:

“The reference to the “level” of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited [sic] to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.”¹³⁹

249. In assessing the level of damage suffered by data subjects, the DPC has had regard to the fact that their personal data was processed without a lawful basis under Article 6 GDPR, and without a condition for the processing of special category data in the form of biometric data under Article 9 GDPR. The DPC has also had regard to the fact that it was a pre-condition of accessing the relevant benefits provided for by law by the DSP that data subjects had to submit to such processing. A core element of the principle of lawfulness for processing is that controllers ensure that they only process personal data that is necessary. Data subjects are denied control over their personal data where a controller processes it in a manner that is not necessary in relation the purposes of the processing.

¹³⁷ Central Statistics Office, “Population and Migration Estimates, April 2021”, <<https://www.cso.ie/en/releasesandpublications/ep/p-pme/populationandmigrationestimatesapril2021/mainresults/>> (Accessed 11 April 2025)

¹³⁸ $3,488,101/5,011,500 \times 100$.

¹³⁹ EDPB Fining Guidelines [53.b.v].

The nature of the infringements

250. The EDPB Fining Guidelines state that the nature of the infringement is “assessed by the concrete circumstances of the case.” In this assessment, the supervisory authority may:

“review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.”¹⁴⁰

251. In line with the text of the GDPR, the nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.¹⁴¹

252. The nature of the infringement of Article 5(1)(a) is a failure to comply with one of the core principles of the GDPR, which requires processing to be lawful, fair and transparent. The infringement of Article 6(1) relates to the DSP unlawfully processing personal data, and the infringement of Article 9(1) resulted in processing that goes against the prohibition in processing special categories of personal data. In the context of the nature, scope and purposes of the processing in this inquiry, the nature of these infringements resulted in the DSP processing special category personal data of 70% of the population of the State without a lawful basis.

253. The infringement of Article 5(1)(e) relates to an infringement of the storage limitation principle, which is a core principle of the GDPR. In the within circumstances, this amounted to unlawful storage of biometric data for a period of the lifetime of data subject.

254. The infringements of Articles 13(1)(c) and 13(2)(a) arose from a failure to provide transparent information to data subjects about lawful bases or retention periods for the processing of personal data to which data subjects are subjected on a mandatory basis as a pre-condition to receiving welfare payments.

255. The infringements of Articles 35(7)(b) and (c) arose from a failure to include all of the required details in the DPIA that the DSP eventually conducted in respect of the

¹⁴⁰ EDPB Fining Guidelines, [53.a].

¹⁴¹ Article 83(2)(a).

processing, which resulted in a failure to identify all of the risks associated with this processing, including the risk that there was no lawful basis for processing.

256. For the reasons expanded upon in relation to each individual infringement above, the DPC considers the infringements identified herein to be of a serious nature.

The gravity of the infringements

257. The gravity (as well as the nature and duration of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.¹⁴²

258. Above, those factors were all considered insofar as they relate to the processing of biometric data conducted by the DSP. The analysis of those factors revealed that the DSP processed special categories of personal data without a lawful basis, without adequate transparency and without conducting a sufficient DPIA. The gravity of these infringements is of a high severity, particularly taking into account the fact that data subjects were required to submit to that processing in order to obtain welfare payments from the State.

The duration of the infringements

259. In relation to the duration of an infringement, the EDPB Fining Guidelines state, *“a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.”*¹⁴³

260. The A29WP Fining Guidelines note that duration may be illustrative of:

- a) wilful conduct on the data controller’s part, or
- b) failure to take appropriate preventive measures, or
- c) inability to put in place the required technical and organisational measures.¹⁴⁴

¹⁴² Article 83(2)(a).

¹⁴³ EDPB Fining Guidelines [53.c].

¹⁴⁴ A29WP Fining Guidelines, p11.

261. The duration (as well as the nature and gravity of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.¹⁴⁵

262. In this case, the duration of the infringements of Articles 5(1)(a), 5(1)(e), 6(1), 9(1), 13(1)(c), and 13(2)(a) commenced at the date of application of the GDPR, 25 May 2018, and are ongoing, as the DSP continues to carry out the processing in scope. The duration of the infringements of Articles 35(7)(b) and 35(7)(c) commenced in February 2020 when the first version of the DPIA was produced.

Assessment of Article 83(2)(a)

263. To summarise the foregoing analysis, the infringements identified herein relate to core principles of the GDPR, the requirement that processing of ordinary and special categories of data be lawful, obligations of transparency and the requirement to conduct a DPIA. They arose from processing to which data subjects were mandatorily subjected in order to receive welfare payments, and which was conducted on the personal data of 70% of the population of the State. Taking account of all of the factors assessed in this section, the DPC assesses the ongoing infringements to have a high gravity and a serious nature.

ii. Article 83(2)(b) GDPR: the intentional or negligent character of the infringement

264. The A29WP Fining Guidelines state,

*“in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas “unintentional” means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.”*¹⁴⁶

265. The EDPB Fining Guidelines state,

“The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is generally admitted that intentional infringements, “demonstrating contempt for the provisions of the law, are more severe than unintentional ones”.¹⁴⁷ In case of an intentional infringement,

¹⁴⁵ Article 83(2)(a).

¹⁴⁶ A29WP Fining Guidelines, p11.

¹⁴⁷ Footnote from EDPB Fining Guidelines: *Guidelines WP 253*, p. 12.

the supervisory authority is likely to attribute more weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.”

266. Examples of intentional conduct outlined in the A29WP Fining Guidelines include explicit authorisation of processing by top management despite advice from the data protection officer or in disregard for existing policies.¹⁴⁸

267. In this case, the DPC finds that the infringements indicate negligence on the part of the DSP. The DSP’s infringements of the GDPR relating to the legal basis and the retention period were done on the belief that the identified legal provisions were a sufficient legal basis. However, the submissions made do not make any reference to the DSP putting its mind to the question of whether or not there was a clear and foreseeable basis from those legal provisions and whether it was necessary and proportionate in the circumstances. The transparency infringements also amounted to a failure to put in place information that the DSP ought to have known should have been provided to data subjects. Additionally, the DSP failed to appropriately account for the clear requirements of Articles 35(7)(b) and 35(7)(c) GDPR.

268. The guidance and law as it relates to these infringements was such as the time as to indicate that the GDPR would be infringed in the absence of a clear and foreseeable, necessary and proportionate legal basis, and therefore likely to result in a high risk to the rights and freedoms of natural persons. Therefore, the DPC is satisfied that the DSP was negligent within the meaning of Article 83(2)(b) GDPR. The DPC considers that this amounted to a high degree of negligence, as a controller in the position of the DSP ought to have been aware of its obligations under the GDPR.

iii. Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects

269. According to the A29WP Fining Guidelines:

“This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.”¹⁴⁹

¹⁴⁸ A29WP Fining Guidelines, p12.

¹⁴⁹ A29WP Fining Guidelines, p12-13.

270. In this case, the DSP has not taken mitigating measures to mitigate the damage suffered by data subjects. However, the DSP has taken the position throughout the inquiry that it has not infringed the GDPR.

iv. Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

271. The key question in relation to this provision is whether the DSP “did what it could be expected to do” given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on the DSP by the Regulation.”¹⁵⁰

272. In this case, the DSP did conduct a DPIA, provide information to data subjects about the processing and consider whether the processing was lawful. However, the DSP has not done everything that would be expected for an organisation of its nature. The DSP is a government department with 6,059 staff as of 2021.¹⁵¹ It would be expected that a public body of that size and prominence would take further appropriate steps than those already outlined to ensure that its processing of personal data was in compliance with the obligations of the GDPR including core principles relating to lawfulness and storage limitation, the obligations of transparency and the requirements of a DPIA.

273. Against this backdrop, the DPC considers that the DSP holds a high degree of responsibility for the infringements because it was within its control to conduct appropriate assessments of the lawfulness of processing and DPIAs, and it could have done more to provide lawful and transparent information to data subjects.

v. Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor

274. In line with the EDPB Fining Guidelines, prior infringements are those already established before the draft decision (in the sense of Article 60 GDPR) is issued.¹⁵²

275. According to the A29WP Fining Guidelines, “[t]his criterion is meant to assess the track record of the entity committing the infringement.”¹⁵³

¹⁵⁰ EDPB Fining Guidelines, [77].

¹⁵¹ Department of Social Protection, “Annual Report 2021”, <<https://www.gov.ie/pdf/?file=https://assets.gov.ie/232047/c27eefe5-789e-4864-b601-d50c85e1bd20.pdf>> (Accessed 11 April 2025)

¹⁵² EDPB Fining Guidelines, [82].

¹⁵³ A20WP Fining Guidelines, p14.

276. In this case, the DSP has not been found to have committed any relevant previous infringements of the GDPR by the DPC or another supervisory authority.

vi. Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

277. The extent to which the DSP has cooperated with the inquiry is relevant to consider under this heading.¹⁵⁴ In this case the DSP has cooperated fully with the inquiry process. However, controllers have a duty to cooperate with supervisory authorities under Article 31 GDPR. Moreover, the cooperation envisaged by Article 83(2)(f) is cooperation for the purposes of remedying the infringement and mitigating the possible adverse effects of the infringement. The DSP has maintained throughout the inquiry that it is not infringing the GDPR and therefore it has not sought to mitigate the adverse effects of the infringement.

vii. Article 83(2)(g) GDPR: the categories of personal data affected by the infringement

278. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringement(s) concern Article 9 or 10 data, whether the data are directly or indirectly identifiable, whether the data are encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.¹⁵⁵

279. The processing relates to biometric data, which is a special category of personal data. Data subjects are directly identifiable from this data, which takes the form of biometric templates of photographs. The processing of this special category data was carried out on a broad scale, and affected 70% of the population of the State. In line with the guidance quoted above, it is relevant to consider the fact that the processing of special category data is in scope.

¹⁵⁴ A29WP Fining Guidelines, p14.

¹⁵⁵ A29WP Fining Guidelines, p14.

viii. Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

280. According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement “as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.”¹⁵⁶

281. In this case, the DPC became aware of the infringements as a result of information that became available to the DPC through a separate pre-GDPR investigation. Nothing further arises in relation to this heading.

ix. Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

282. The A29WP Fining Guidelines state

“As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors “with regard to the same subject matter””.¹⁵⁷

283. Previous measures have not been ordered under Article 58(2) GDPR against the controller, therefore, nothing further arises for consideration here.

x. Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

284. No relevant codes of conduct or certification mechanisms are applicable here. Therefore, nothing further arises for consideration under this heading.

¹⁵⁶ A29WP Fining Guidelines, p15.

¹⁵⁷ A29WP Fining Guidelines, p15.

- xi. **Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement**

285. Nothing further arises under this heading.

- xii. **Decision as to whether to impose a fine**

286. The decision to impose an administrative fine “needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.”¹⁵⁸

287. Taking into account the assessment of the criteria at (a) to (k) above, the DPC proposes to impose administrative fines for the infringements of the GDPR identified in this Decision.

288. The infringements are of a serious nature and a high degree of gravity. They affect the personal data of a number of data subjects equal to 70% of the population of the State. The infringements relate to a special category of personal data and include infringements of core GDPR principles, the overall lawfulness of the processing, and failures to conduct a DPIA and to provide transparent information.

289. Considering the degree of severity of these infringements, the scope of processing, the fact that the DSP was found to have been negligent and to have a high degree of responsibility for the infringements, the DPC considers that this wrongdoing should be sanctioned by the imposition of administrative fines.

b) Decision on the amount of the administrative fine

290. Above, it was determined that it was necessary to impose an administrative fine. This section calculates the amount of that fine, taking into account the methodology required to be applied by the EDPB Fining Guidelines, based on the assessments of the individual Article 83(2) GDPR criteria that are recorded above.

- i. **Article 83(3) GDPR**

291. In accordance with Article 83(3) GDPR:

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

¹⁵⁸ EDPB, Binding Decision 1/2023.

292. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. all of the processing operations that the DSP carries out on biometric personal data in the context of SAFE 2 registration.

293. In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR which was set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.¹⁵⁹

294. The relevant passage of that binding decision is as follows:

“315. All CSAs argued in their respective objections that not taking into account infringements other than the “gravest infringement” is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

316. The EDPB notes that the IE SA identified several infringements in the Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

¹⁵⁹ Inquiry IN-18-12-2.

318. In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.

319. Article 83(3) GDPR reads that if “a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.”

320. First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from “the same or linked processing operations”.

321. The EDPB highlights that the overarching purpose of Article 83 GDPR is to ensure that for each individual case, the imposition of an administrative fine in respect of an infringement of the GDPR is to be effective, proportionate and dissuasive. In the view of the EDPB, the ability of SAs to impose such deterrent fines highly contributes to enforcement and therefore to compliance with the GDPR.

322. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the *effet utile* principle requires all institutions to give full force and effect to EU law. The EDPB considers that the approach pursued by the IE SA would not give full force and effect to the enforcement and therefore to compliance with the GDPR, and would not be in line with the aforementioned purpose of Article 83 GDPR.

323. Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

324. With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording “amount specified for the gravest infringement” refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of

the Regulation 2016/679 state that the "occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

325. The wording "total amount" also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording "total amount" in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine. 327. In light of the above, the EDPB instructs the IE SA to amend its Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness."

295. The impact of this interpretation is that administrative fine(s) are imposed cumulatively, as opposed to imposing only the proposed fine for the gravest infringement. The only applicable limit for the total fine imposed, under this interpretation, is the overall "cap". By way of example, in a case of multiple infringements, if the gravest infringement was one which carried a maximum administrative fine of 2% of the turnover of the undertaking, the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

296. In this case, infringements were identified of Articles 5(1)(a), 5(1)(e), 6(1), 9(1), 13(1)(c), 13(2)(a), 35(7)(b) and 35(7)(c) GDPR. The gravest infringement is that of Article 5(1)(a) GDPR, considering that this is a core principle of the GDPR affecting the overall lawfulness of processing.

ii. Categorisation of the infringements under Articles 83(4)-(6) GDPR

297. Articles 83(4)-(6) GDPR indicate the degrees of seriousness accorded to different categories of infringement. The EDPB Fining Guidelines note that:

“With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.”

298. The categorisation of the infringements under Articles 83(4) or (5) is a relevant consideration in assessing the seriousness of the infringements in this case. The infringements of Articles 5(1)(a), 5(1)(e), 6(1), 9(1), 13(1)(c), and 13(2)(a) found in this case are ascribed considerably greater significance, with the legislator for, in general, maximum administrative fines double those applicable to the infringements of Articles 35(7)(b) and 35(7)(c).

iii. Seriousness of the infringement pursuant to Articles 83(2)(a), (b) and (g) GDPR

299. The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the seriousness of the infringement.¹⁶⁰ These factors were assessed above. The guidelines also state that:

“This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.”¹⁶¹

300. Having regard to these factors as a whole, the infringements identified in this case are of a high seriousness. Under Article 83(2)(a) the infringements were found to be of a serious nature and have a high degree of gravity. In relation to Article 83(2)(g), it was found that the infringements affected the special category data of millions of data subjects, including children and vulnerable adults, and the DSP was found to have acted negligently with respect to these infringements in line with Article 83(2)(c).

301. As the infringements are of a high level of seriousness, the starting point for calculation is between 20 and 100% of the applicable maximum.

¹⁶⁰ EDPB Fining Guidelines, [51].

¹⁶¹ EDPB Fining Guidelines, [59].

iv. Imposing an effective, dissuasive and proportionate fine

302. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this doesn't "*dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.*"¹⁶² Article 83(1) will be considered again at the end of this calculation.

v. Aggravating and mitigating circumstances

303. Articles 83(2)(a), (b) and (g) GDPR were considered above in relation to the starting point for the calculation of the fine. In line with the approach suggested in the EDPB Fining Guidelines,¹⁶³ this section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR.

304. In relation to Article 83(2)(c), it was noted that the DSP had not adopted measures to mitigate the damage to data subjects. This factor is considered to be neither mitigating nor aggravating.

305. In relation to Article 83(2)(d), it was noted that the DSP had a high degree of responsibility for the infringements. This is considered an aggravating factor of moderate weight, considering that it is a public body that ought to have known that its practices infringed the GDPR. Considering that the DSP did take some steps to seek to ensure compliance, including providing information to data subjects and conducting a DPIA, the weighting attributed to this factor is moderate rather than high.

306. In relation to Article 83(2)(e), it was noted that the DSP did not have any previous relevant infringements. This factor is considered to be neither mitigating nor aggravating.

307. In relation to Article 83(2)(f), it was noted that the DSP had cooperated with the DPC throughout the inquiry. The cooperation did not have the effect of mitigating the damage to data subjects, as the DSP maintained that throughout the inquiry it had not infringed the GDPR. The DSP also has a general obligation to cooperate under Article 31 GDPR. In line with these considerations, this factor is considered to be neither mitigating nor aggravating.

¹⁶² EDPB Fining Guidelines, [64].

¹⁶³ EDPB Fining Guidelines, [70].

308. In relation to Article 83(2)(h), it was noted that the manner in which the infringement became known to the DPC was through a previous, pre-GDPR investigation. This factor is neither mitigating nor aggravating as it related to a different legal regime.
309. In relation to Article 83(2)(i), it was noted that orders had not been previously ordered by the DPC¹⁶⁴ with regard to the same subject matter. This factor is considered to be neither mitigating nor aggravating.
310. In relation to Article 83(2)(j), it was found that there were no relevant approved codes of conduct or approved certification mechanisms for consideration. This factor is neither mitigating nor aggravating.
311. In relation to Article 83(2)(k), it was noted that there were no additional aggravating or mitigating factors for consideration. This factor is neither mitigating nor aggravating.
312. Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2) together with the requirements of the Fining Guidelines, as detailed above, the DPC imposes fines totalling €550,000, as broken down below:
- a. For the infringement of Article 5(1)(a) GDPR, a fine of €140,000.
 - b. For the infringement of Article 6(1) GDPR, a fine of €110,000.
 - c. For the infringement of Article 9(1) GDPR, a fine of €110,000.
 - d. For the infringement of Article 5(1)(e) GDPR, a fine of €60,000.
 - e. For the infringements of Articles 13(1)(c) and 13(2)(a) GDPR, a fine of €90,000.
 - f. For the infringements of Articles 35(7)(b) and (c) GDPR, a fine of €40,000.

vi. The relevant legal maximums for administrative fines

313. The DPC notes that the DSP as a Department of State is a public authority as defined in section 2(1) of the 2018 Act. Section 141(4) of the 2018 Act provides that any administrative fine that the DPC decides to impose on a public authority or public body shall not exceed €1,000,000 unless that authority or body acts as an undertaking within the meaning of the Competition Act 2002. As the administrative fines imposed in this

¹⁶⁴ Paragraph 101 of the EDPB Fining Guidelines says “as opposed to Article 83(2)(e) GDPR, this assessment only refers to measures that supervisory authorities themselves have previously issued to the same controller or processor with regard to the same subject matter”.

Decision do not exceed that amount, it is not necessary for the DPC to determine whether the DSP acts as an undertaking for the purpose of the processing concerned.

vii. Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness

Effectiveness

314. It is the DPC's view that for a fine to be effective, it must be large enough to have a significant effect on the controller or processor such that GDPR compliance, motivated by avoiding such fines in the future, becomes a factor in the entity's governance and management decision-making at the highest level. Furthermore, a sufficiently large fine is necessary to ensure that the fine is not a mere insignificant expense for the controller or processor concerned, and to ensure that the entity does not enjoy an unfair advantage by its ability to absorb even large fines for its infringements of the GDPR.

315. It is the DPC's view that the fine above is effective. The proposed fines amounts to over 50% of the maximum fine that can be imposed on a public body, underscoring the seriousness of the infringements that have been identified herein. The DPC considers this to be an effective fine for the purposes of sanctioning such non-compliance with the GDPR.

Dissuasiveness

316. In order for a fine to be "dissuasive", it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. The DPC considers that the proposed are dissuasive for both. The DPC considers the monetary value of the proposed fines to be sufficient to have such a deterrent effect.

317. As previously noted, each of the infringements is both serious in nature and ongoing. The DPC considers that the DSP's non-compliance with its obligations under the above-referenced GDPR provisions must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of data subjects whose personal data, including biometric data, are processed in connection with the allocation of a PSC. Therefore, the DPC considers that the administrative fines are appropriate and necessary to dissuade non-compliance.

Proportionality

318. Proportionality is a principle of EU law that requires a measure to pursue a legitimate objective, be appropriate to attain that objective, and not go beyond what is necessary to achieve the objective. The objectives of the administrative fines in this case

are to both re-establish compliance with the rules, and to sanction the DSP's infringements. As regards the requirement for any fine to be necessary to these objectives, this requires the DPC to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

319. The DPC considers that the fines proposed above are proportionate. The infringements identified in this Decision are of a serious nature and a high degree of gravity. The DSP was found to have a high degree of responsibility for those infringements and to have acted negligently with regard to their commission. The infringements relate to core principles of data protection law, and the DSP did not do what it ought to have done to ensure that its processing was in compliance with the requirements to have a lawful basis for processing, to provide transparent information to data subjects and to conduct a DPIA.

320. Having regard to those considerations, which have been elaborated upon throughout the analysis in this section and throughout this Decision, the DPC is satisfied that the fines are no greater than required to enforce compliance in respect of the infringements identified in this Decision.

M. SUMMARY OF ENVISAGED ACTION

321. In summary, the corrective powers that the DPC will exercise are:

- a. An order pursuant to Article 58(2)(f) GDPR to the DSP to cease the processing of biometric data in the SAFE 2 registration process effective 9 months from the date of notification of the final decision if the DSP does not identify a valid lawful basis;
- b. A reprimand to the DSP pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and
- c. Administrative fines totalling €550,000.

N. RIGHT OF APPEAL

322. This Decision is issued in accordance with section 111 of the 2018 Act. Section 150(5) gives a person affected by a legally binding decision of the DPC a right of appeal within 28 days from the date on which notice of that Decision is received by it.

Dale Sunderland
Commissioner for Data Protection