In the matter of the General Data Protection Regulation

DPC Case Reference: IN-22-7-3

In the matter of Permanent TSB plc trading as PTSB and PTSB Asset Finance

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

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

DECISION

Decision-Makers for the Data Protection Commission:

_____

Dr Des Hogan, Commissioner for Data Protection
&
Mr Dale Sunderland, Commissioner for Data Protection

30 April 2026

Data Protection Commission
6 Pembroke Row
Dublin, D02 X963
Ireland

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

A. Introduction

1. The General Data Protection Regulation ('**GDPR**') is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018.[1]

2. The Data Protection Commission ('**the DPC'**) was established on 25 May 2018, pursuant to the Data Protection Act 2018 ('**the 2018 Act**'), as Ireland's supervisory authority within the meaning of, and for the purposes specified in, the GDPR.[2]

3. The GDPR elaborates on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in the Charter of Fundamental Rights of the EU ('**the Charter**') and Article 8 in particular, which safeguards the protection of personal data provides:

    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.

4. This document ('**the Decision**') is a decision made by the DPC in accordance with section 111 of the 2018 Act. The DPC makes this Decision having considered the information obtained in an own-volition inquiry ('**the Inquiry'**) pursuant to section 110 of the 2018 Act.

5. This Decision considers particular aspects of the fundamental right to the protection of personal data in relation to the security of processing and compliance with responsibilities arising when a personal data breach has occurred.

---

[1] Reference to 'the GDPR' in this Decision is to Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC ('**General Data Protection Regulation**').

[2] SI 175/2018 Data Protection Act 2018 (Establishment Day) Order 2018.

6. This Decision is being provided to Permanent TSB plc trading as PTSB and PTSB Asset Finance ('**PTSB**') pursuant to section 116(1)(a) of the 2018 Act, in order to give notice of the Decision, the reasons for it, and the decision in relation to the powers exercised pursuant to Article 58 of the GDPR.

7. This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) GDPR arising from the infringements that have been identified herein. It should be noted in this regard that PTSB is required to comply with the corrective powers that are contained in this Decision, and it is open to the DPC to serve an enforcement notice on PTSB in accordance with section 133 of the 2018 Act.

B. Preliminary Matters

a) Data Controller

8. In commencing the Inquiry, the DPC considered that PTSB was the controller, within the meaning of Article 4(7) GDPR, in respect of the processing of personal data that was the subject of the personal data breach notifications relevant to Inquiry (and detailed below). In this regard, PTSB had confirmed that it was the controller in its breach notifications of 26 and 27 May 2022.

b) Factual Scope of the Inquiry

9. This Inquiry was commenced following a series of three data breach notifications made by PTSB to the DPC on 26 and 27 May 2022. These notifications were logged on the DPC system as BN-22-5-459, BN-22-5-469, and BN-22-5-497 ('**the Breaches**') and concerned PTSB's processing of personal data – including financial data – through its 'Open24 Contact Centre'.

10. PTSB is a leading provider of personal and business banking services in the Irish market. The Open24 Contact Centre functions as PTSB's primary point of customer contact. The Open24 Contact Centre receives a large volume of calls from customers seeking to take action in relation to their accounts, such as checking their account balance, transactions, standing orders or to make fund transfers and payments to other designated accounts. In this respect, PTSB has advised that the Open24 Contact Centre received circa [redacted] calls during 2022 and that PTSB recruited and trained [redacted] Open24 Contact Centre staff in the same period.[3] The quantity of personal data potentially stored on customer accounts

[3] PTSB response to Statement of Issues 24 February 2024 p1-2.

is also broad in scope and sensitive in nature, including data subject identity, contact details, and economic and/or financial data.

11. The Breaches each concerned circumstances where malicious actors, in possession of certain customer information, called PTSB's Open24 Contact Centre posing as those customers and sought to access their accounts or obtain or amend account details. PTSB stated in its submissions of 12 September 2022 that the same source phone number was used in BN-22-5-469 and BN-22-5-497. It is therefore highly likely that the same malicious actor was behind both attacks.[4] The source number differed in BN-22-5-459 and PTSB stated that this attack "*appears to have involved a different bad actor*".[5] In all three instances, PTSB agents repeatedly failed to follow security procedures and the malicious actor was able to change the mobile phone number on the accounts. Other information [redacted] were also disclosed by PTSB due to security failings. This meant that data subjects were put at increased risk of additional fraud, were forced to close their accounts and in BN-22-5-497 and BN-22-5-469, data subjects suffered financial loss. In the context of BN-22-5-497, the correct security procedures were not followed on at least five calls with five separate agents.[6] Similarly, in the context of BN-22-5-469, appropriate procedures were not followed on at least three separate occasions leading to the occurrence of repeated personal data breaches.

12. Article 4(12) GDPR defines a data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". As the Breaches involved the unauthorised alteration, disclosure of and access to personal data processed by PTSB related to data subject accounts, the DPC is satisfied that personal data breaches occurred under the meaning provided by Article 4(12) GDPR.

13. Three data subjects were affected by the Breaches, however, as the Breaches concerned the technical and organisational measures implemented by PTSB in the Open24 Contact

[4] PTSB response to commencement Notice 12 September 2022 p40.
[5] PTSB response to commencement Notice 12 September 2022 p40.
[6] In its submissions PTSB referred to agents and staff in relation to persons working on the behalf of PTSB. PTSB also confirmed that agents are "*bound by the same rules for securely identifying customers as full-time employees*" as noted at paragraph 28. Throughout this decision the DPC interchangeably uses agent and staff to refer to those persons working on behalf of PTSB.

Centre, and the organised use of social engineering by bad actors seeking to circumvent those measures, a potentially much higher number of data subjects were put at risk and could have been affected.

C. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

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

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

b) Legal Basis for the Decision

16. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act. This 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. In so doing, the DPC is required to assess all of the materials and submissions gathered during the Inquiry and any other materials which the DPC considers to be relevant, in the course of the decision-making process.

17. 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. The DPC has had regard to submissions made by PTSB in respect of the draft version of this Decision sent to PTSB on 29 August 2025 (‘**the Draft Decision’**) before proceeding to make this final Decision under section 111 of the 2018 Act.

D. Factual Background

18. PTSB is a provider of banking services in Ireland, having its registered office at 56-59 St. Stephen's Green, Dublin 2. PTSB provides banking services via *inter alia* the Open24 service. The Open24 service is defined as "*the system provided by [PTSB] from time to time to enable Customers and their Users to access, transact, and utilise services provided by us using telephone, Internet or other technology-based communication*."[7] The Open24 Contact Centre is PTSB's primary point of customer contact and sits within PTSB's Digital and Direct Team. It provides PTSB customers with access to a range of banking services via telephone.

19. As noted above, the data breach notifications each concerned circumstances where a malicious actor, in possession of certain customer information, called PTSB's Open24 Contact Centre posing as those customers and seeking to access their accounts or obtain or amend account details. Based on the analysis undertaken of the breach notifications and subsequent documentation provided during the breach handling process, the DPC considered that the matters concerned breaches of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by PTSB and thus constituted personal data breaches within the meaning provided by Article 4(12) GDPR.

20. Following its own review, the DPC was of the opinion that one or more provisions of the 2018 Act and/or the GDPR may have been contravened in this case. The DPC subsequently commenced an Inquiry of its own volition under, and in accordance with, section 110(1) of the Act on 24 August 2022.

21. The circumstances of each of the Breaches are outlined below.

BN-22-5-459

22. In the breach notification form for BN 22-5-459, dated 26 May 2022, PTSB advised that the data breach concerned a confidentiality breach (i.e. unauthorised disclosure of or access to personal data) and an integrity breach (i.e. alteration of data) concerning an incident which occurred on 8 April 2022.

23. A bad actor contacted the Open24 Contact Centre by phone on 8 April 2022 and successfully changed the mobile phone number associated with the customer's account. PTSB stated that the customer's online banking access and Visa debit card for his sole-owner current account were cancelled on 8 April 2022 after he advised PTSB via telephone

[7] Open24 Online Banking Terms and Conditions, p3.

that he had fallen victim to a vishing fraud incident on the same day.[8] In a response provided to the DPC of 22 June 2022, PTSB noted that this was an error and the customer had in fact fallen victim to a smishing fraud incident.[9]

24. On 16 April 2022, the customer called PTSB again and advised that he was having difficulty completing transactions from a different, joint-owner current account also held with PTSB. PTSB concluded that the incorrect phone number was held on file and that the customer had not received the secure customer authentication text messages. Upon further investigation, PTSB determined that the phone number on file had been updated by a malicious actor on 8 April 2022 and this incorrect number remained on the account until 16 April 2022. PTSB stated that the update occurred due to the bank's agent's failure to follow security procedures properly. In a subsequent phone call received by a separate service agent on 8 April 2022, the customer's email address was verbally disclosed to the fraudulent caller. This was despite the caller's failure to satisfactorily answer the designated security questions.

25. PTSB noted that it was protocol for an SMS message to issue [redacted] as a means of verifying that the number was not updated fraudulently or in error. In this instance PTSB noted that the customer did not have a record of receiving this notification; however, PTSB stated that it held a record confirming that the SMS had issued.

26. PTSB indicated that remedial mitigating measures were put in place after the breach, including:

> *"1. Feedback has been provided to the relevant department.*
>
> *2. The customer's phone number has been reverted on the Bank's systems.*
>
> *3. The customer's online access number and Visa debit cards have been cancelled.*
>
> *4. The Bank has recommended the customer close his accounts with the Bank as the Bank would no longer be in a position to continue to guarantee the safety of the account in the future. In the meantime, transaction holds have been placed on the customer's accounts in an effort to prevent any fraudulent activity on the accounts.*

[8] Vishing is the use of fraudulent phone calls to make the recipient provide his or her personal data to the bad actor.
[9] Smishing is the use of fraudulent text messages, including SMS or instant messages, to make the recipient provide his or her personal data to the bad actor.

5. The staff members responsible for this security breach were removed from customer calls and provided with emergency training, outlining the Bank's security procedures.

6. An email reminding all staff in the Bank's contact centre of the correct security procedures has been issued."

27. Subsequent to the breach notification BN 22-5-459, the DPC wrote to PTSB on 1 June 2022 seeking further information in relation to the breaches.

28. PTSB responded on 8 June 2022 and confirmed that the call by the malicious actor on 8 April 2022 was handled by an agent contracted to work for PTSB and based in the PTSB call centre. PTSB confirmed that such agents were "*bound by the same rules for securely identifying customers as full-time employees*".

29. PTSB additionally provided the following details in relation to the protocols and procedures for verification of callers' ID and changing customers' contact phone numbers.

[redacted]

[redacted][10]

30. PTSB confirmed that there was no written protocol in place to notify a manager or to place an alert after unsuccessful attempts to change the contact telephone number of a customer. However, for agent assisted calls, it was procedure [redacted]

31. PTSB provided the following response in relation to the DPC's query regarding the protocols, procedures or rules governing the internal reporting of personal data breaches to PTSB's Data Protection Unit:

> *"As per PTSB data breach protocol all incidents of loss of control of personal data must be reported to the DP team as soon as staff become aware of the incident. Staff members must promptly report any breach to their Line Manager and/or Head of Function and the Data Protection team within 24 hours of detection. If there are other circumstances where a data breach or suspected data breach occurred, staff members are asked to contact the Data Protection Team. If, on review, the Data Protection team determines that a breach has occurred, the Data Protection team will then advise whether: -*
>
> *the breach needs to be reported to the DPC; and*
>
> *the affected data subject/individual needs to be informed of the breach"*

32. The DPC team handling the breach notification wrote to PTSB on 15 June 2022 seeking further information in relation to the breaches. On 22 June 2022, PTSB responded to the DPC and indicated that there was an error in its submission on 26 May 2022, whereby it had indicated that the customer had fallen victim to a vishing fraud incident and that it was in fact a smishing fraud incident. PTSB confirmed that this occurred on 8 April 2022, when the customer received a text message purporting to be from his mobile service provider and clicked on a link. The customer then contacted PTSB's fraud department on the same date to advise them of the matter and provided his name, address, BIC, IBAN & card details in relation to the account held in his sole name. PTSB confirmed that customer's personal

[10] The response provided by PTSB on 8 June 2022 was subsequently corrected by PTSB in its submissions of 16 February 2024 due to a number of factual inaccuracies. The updated information appears in the quote.

online access and debit card for his sole account were both cancelled by PTSB on 8 April 2022, following the above referenced telephone call.

33. PTSB additionally provided the below response in relation to the DPC's query as to whether the protocols or procedures in effect at the time of those cancellations require or advise placing restrictions or security flags on other accounts of the customer:

> *"[O]nce the Bank became aware of the smishing incident where the customer provided details of the account held in his sole name, his personal online access and debit card for his sole account were cancelled. At the time of the smishing incident, the details provided by the customer to the fraudulent actor were not deemed severe enough to warrant additional action across all accounts.*
>
> *It was regrettable that as a result of the agent disclosures, that the customer's mobile phone number was provided to the unauthorised party which led to an amendment of this number on our customer's records. It was this reason why the customer experienced difficulty in completing transactions on his joint account as the secure customer authentication text messages were not being received by him, which is how this matter came to light. The Bank then took additional action by placing transaction holds [restricts transactions] on both the sole account and the account held in joint names."*

34. In its submissions of 16 February 2024 on the DPC's Issues Paper, provided as part of the Inquiry,[11] PTSB stated that while the agent did not follow security protocols, and while the customer's number was amended on its records as a result, the agent did not in fact disclose the customer's phone number.

BN-22-5-469

35. In the breach notification form for BN-22-5-469, dated 27 May 2022, PTSB advised the DPC that the data breach concerned a confidentiality breach (i.e. unauthorised disclosure of or access to personal data), an integrity breach (i.e. alteration of data), and an availability breach (i.e. loss or destruction of data).

36. PTSB stated that on 3 May 2022 a customer contacted PTSB to query fraudulent transactions on her current account. On reviewing the customer's account, PTSB noted that a malicious actor had called the Open24 Contact Centre on three consecutive days from 20

[11] DPC Inquiry Issues Paper was issued to PTSB on 18 January 2024. It was intended to document the relevant facts established by the DPC and the issues which might fall for consideration in the decision of the DPC.

April 2022. PTSB stated that the malicious actor provided [redacted] for the customer account. However, PTSB call agents repeatedly failed to follow proper security protocol and disclosed customer details on these calls [redacted] These details allowed [redacted] the bad actor to access the customer's account and make a number of fraudulent transactions totalling approximatively €35,000.[12]

37. PTSB further stated that during a call on 22 April 2022, the bad actor was successful in updating the mobile phone number registered to the Open24 account despite failing to satisfactorily complete the relevant security protocol. This phone number is required for secure customer authentication for online transactions. PTSB issued an SMS [redacted] to ensure that the change had not been carried out fraudulently or in error. The customer subsequently confirmed receipt of the SMS but did not contact PTSB at the time as they were resident in [redacted]

38. PTSB said that its fraud monitoring system was triggered on 22 April 2022 in relation to one of the fraudulent transactions. However, the phone number on the account had been updated at this point, which resulted in the bad actor being contacted in relation to the transaction. The bad actor falsely confirmed that the queried transaction was genuine. On 3 May 2022 the customer called the fraud department and the extent of the fraudulent activity was established.

39. Subsequent to the breach notification BN 22-5-469, the DPC team handling the breach notification wrote to PTSB seeking further information in relation to the breaches. In particular, the DPC requested clarification as to how the contact number for the customer's account was changed by the bad actor without confirmation being received in response to the SMS notification sent to the customer in [redacted]

40. PTSB responded on 8 June 2022 and clarified, *inter alia*, as below:

> *"In circumstances where a phone number is updated on an account, it is protocol for an SMS notification message to issue* [redacted] *as a means of verifying that the number was not updated fraudulently or in error. This SMS message, which is intended as a security measure and requests that the*

[12] A full refund was later made available to the customer on 27 June 2022.

customer 'contact us if this update was not made by you', does not require confirmation by return. This change is made at the point of time at which the amendment to the account is made. In this instance, as the customer did not contact the bank as a result of this SMS notification, the amendment to the account remained in place until the customer called the bank directly on 3 May 2022."

41. In its submissions of 16 February 2024 on the Issues Paper, PTSB clarified that there is a [redacted] delay in the new mobile phone number becoming effective to allow time for the customer to respond to the SMS, e.g. a new beneficiary cannot be set up until after the [redacted] have elapsed.[13]

BN-22-5-497

42. In the breach notification form for BN-22-5-497, dated 27 May 2022, PTSB advised that the data breach concerned a confidentiality breach (i.e. unauthorised disclosure of or access to personal data), an integrity breach (i.e. alteration of data), and an availability breach (i.e. loss or destruction of data).

43. PTSB stated that its fraud department noted suspicious transactions on the customer account on 7 May 2022. PTSB attempted to contact the customer to query these transactions but was initially unsuccessful. The customer subsequently contacted PTSB on 9 May 2022 and confirmed that the transactions were fraudulent. On review of the customer's account activity, PTSB noted that a malicious actor had contacted PTSB on four occasions between 6 and 7 May 2022. The unauthorised third party was able to provide the customer's [redacted] The unauthorised third party was provided with the [redacted] due to security failings by PTSB agents. In this instance, the customer did not have a record of receiving an SMS notification when the number was updated, however PTSB stated that it held a record which confirmed that the SMS had issued.

44. PTSB stated that a fraudulent phone number was associated with these accounts from 6 May to 10 May 2022 and that this resulted in an unauthorised third party having access to the customer's account. A number of unauthorised transactions in the amount of

[13] In its submissions of this date, PTSB further noted that, in higher risk jurisdictions, the usual time lag on any changes taking effect has been extended [redacted].

approximately €10,000 were made by the unauthorised third party.[14] PTSB placed transaction holds on the customer's accounts on 9 May 2022 and the customer's phone number was reverted on the bank's systems.

45. PTSB provided details of mitigating measures that were implemented following the breach:

> *"1. Feedback has been provided to the relevant department.*
>
> *2. The fraudulent phone number has been removed from the Bank's systems.*
>
> *3. The customer's online access number has been cancelled.*
>
> *4. The staff members responsible for this security breach were removed from customer calls and provided with emergency training, outlining the Bank's security procedures.*
>
> *5. An email reminding all staff in the Bank's contact centre of the correct security procedures has been issued.*
>
> *6. The Bank placed transaction holds on the customer's accounts on 9 May 2022"*

46. Subsequent to the breach notification BN 22-5-497, the DPC wrote to PTSB on 1 June 2022 seeking further information in relation to the breaches and in particular queried: (i) how the malicious actor in this case gained access to the customer's [redacted];(ii) how the malicious actor came to be given the customer's [redacted] given that these would normally be expected to be known by customers; (iii) if applicable protocols and procedures, or any other rule or practice in effect at the relevant time, required or advised placing an alert or warning on a customer's account after unsuccessful attempts to access customer accounts details by phone; (iv) if the verification SMS message concerning the change of contact phone number was sent to the customer [redacted]

47. PTSB responded on 8 June 2022. In relation to the query as to how the malicious actor gained access to the customer's [redacted] PTSB stated:

> *"Further investigations of the calls received by the Bank have shown that the customer's [redacted][] was disclosed by the Bank's agent. Regrettably, this was due to a failure on the part of the Bank's agent to properly follow the security procedures in place. This information was obtained by malicious actor posing as*

[14] A full refund was provided on 9 June 2022.

the customer by completing some security questions and proceeding through the Open24 registration process in a call on 6 May 2022."[15]

48. As to how the malicious actor came to be given the customer's [redacted], PTSB confirmed:

> *"In this case our records show that regrettably the agent did not follow proper procedure and disclosed the customer's* [redacted] *We can confirm that due to security failings by the Bank's agents, over the course of four calls made between the 6 and 7 May 2022 the unauthorised third party was provided with our customer's* [redacted]*."*

49. PTSB additionally confirmed that its records showed that a verification SMS was sent to the customer [redacted].

E. Scope of the Inquiry and the Application of the GDPR

50. The scope of the Inquiry, which was set out in the Inquiry Commencement Notice which issued on 24 August 2022, was to examine whether or not PTSB discharged its obligations in connection with the subject matter of the notified personal data breaches and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by PTSB in that context.

51. The Inquiry Commencement Notice specified that the Inquiry would focus on PTSB's organisational and technical measures in place to ensure security of the personal data particularly in relation to its telephone call handling processes. In this regard, the Inquiry would examine associated policies and procedures that were in place that identify any risks to data subjects and the organisational and technical measures to address those risks. The Commencement Notice additionally stated that the Inquiry would focus on the areas of Data Protection Governance, Training and Awareness, Records Management and Security of Personal Data. The Commencement Notice also specified that the Inquiry would consider PTSB's compliance with the Article 33 GDPR obligations regarding notification of a personal data breach to the supervisory authority.

52. The temporal scope ('**temporal scope'**) of the Inquiry concerns the period from 25 May 2018 to 27 May 2022.

[15] The response provided by PTSB on 8 June 2022 was subsequently corrected by PTSB in its submissions of 16 February 2024 due to a factual inaccuracy. The updated information appears in the quote.

F. Issues for Determination

53. Having reviewed the Issues Paper and the other relevant materials, the DPC considers that the issues on which it must make a decision are as follows: (i) whether PTSB has infringed Articles 5(1)(f) and 32(1) GDPR in respect of its processing of personal data via the Open24 Contact Centre and (ii) whether PTSB complied with the requirement, under Article 33(1) GDPR, to notify personal data breaches to the DPC without undue delay when notifying the Breaches.

G. Analysis of the Issues for Determination

a) Issue 1: Articles 5(1)(f) and 32(1) GDPR

54. Article 5 GDPR sets out principles relating to processing of personal data. Article 5(1)(f), which relates to the '*integrity and confidentiality'* of personal data, establishes security of personal data processing as one of these core principles.

55. Article 5(1)(f) GDPR states, in this regard, that personal data shall be:

> *"…processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

56. Similarly, Recital 39 GDPR provides that:

> "*Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing*."

57. The security principle in Article 5(1)(f) GDPR is closely associated with Article 32 GDPR. Article 32(1) GDPR provides as follows:

> *""1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

58. Article 32(2) GDPR provides:

"In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

59. Those requirements are reflected in Recital 83 GDPR, which states:

"In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."

60. Arising from the above, it is useful to outline a number of matters which are relevant to the interpretation of Article 5(1)(f) and Article 32 GDPR.

61. First, it is clear that assessment of risk is an important concept in Article 5(1)(f), Article 32(1) and Article 32(2) GDPR. Recitals 75 and 76 GDPR also provide guidance as to the types of risk that can arise from data processing and how risk should be evaluated. In particular, Recital 76 of the GDPR indicates that:

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

62. Second, Article 5(1)(f) GDPR refers to the requirement for a controller to ensure appropriate security of the personal data, using appropriate technical and organisational measures. The GDPR does not identify specific technical and organisational measures that must be applied, nor does it set requirements in terms of the standard of such measures, provided that they are appropriate. Likewise, Article 32 GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from the processing. Whereas that provision does not specify particular measures which should be implemented, the chosen technical and organisational measures should be effective and appropriate in terms of implementing data protection into the processing.[16]

63. Third, Article 32(1)(a) to (d) GDPR provide certain examples of security measures which may be considered in the context of Article 32, and so provides useful guidance as to the types of measures which may be appropriate depending on the processing concerned.

64. For the purpose of assessing PTSB's compliance with Article 5(1)(f) and Article 32 GDPR, the primary issue for consideration is whether the technical and organisational measures which PTSB implemented in respect of the Open24 Contact Centre ensured "*appropriate security of the personal data*", and in particular "*a level of security appropriate to the risk*" arising from the processing. In order for PTSB to comply with Article 5(1)(f) or 32 GDPR, it was not under an obligation to eliminate all risk of a personal data breach occurring, and a strict liability standard is not imposed by the GDPR.

65. Article 32 GDPR in particular requires an assessment of the risks that are presented by the processing, taking into account its nature, scope, context and purpose. Controllers must also consider the risks for the rights and freedoms of data subjects. Having taken these factors into account, the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

i. Assessment of the Risks

66. The processing of personal data by PTSB in the context of its Open24 Contact Centre involves a variety of risks. Those risks include the risk of the loss of access to user accounts as well as unauthorised access and unauthorised disclosure of personal data to third parties. This carries very significant risks for data subjects, including potential misuse of data in the form of unauthorised access leading to financial loss or the disclosure of data

[16] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and Default Guidelines, pages 6-7.

leading to potential identify theft and loss of control over personal data. Furthermore, there is a possibility of users being locked out of their accounts, meaning they no longer have access to the funds contained therein for a period of time, or are required to close their accounts.

67. The requirement in Article 32 GDPR (and Article 5(1)(f) GDPR) is that a controller must assess the risks, or potential threats, associated with the processing of personal data in determining the appropriate level of security to be applied. The purpose of assessing risk, therefore, is to identify potential issues that could arise and the likelihood of same, and put appropriate measures in place to prevent, or minimise the risk of, such issues materialising, whether such occurrences arise unintentionally or otherwise.

68. In considering the risk assessment in the context of Articles 5(1)(f) and 32 GDPR, it is necessary to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. Hence, the risk assessment for PTSB's processing of personal data should have considered, first, the likelihood of unauthorised disclosure or alteration of, or access to, the personal data, and second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments should have been made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data.

69. The assessment within this section of the Decision is concerned with how PTSB evaluated the risk arising in respect of the security of personal data and, in particular, the risk arising from the Open24 Contact Centre as PTSB's primary point of customer contact. In particular, the risk of fraud as a result of an insufficient level of security would severely undermine a customer's relationship with the bank as the relationship is premised on the agreement that the bank would ensure the customers' monies are secure and safe. In addition, the risks posed to vulnerable users are particularly high. Such persons may lack the capacity to realise they have been subject to fraud or financial theft.

70. As regards how PTSB evaluated risk arising in respect of the security of personal data in the Open24 Contact Centre, PTSB outlined that, in its Operational Risk Management

Framework which was approved in December 2020 and implemented in January 2021, it had taken into consideration:[17]

(i) the type of information which is processed via Open24,

(ii) the function of Open24 (front line contact centre) and its limitations (some customer requests cannot be accommodated via Open24),

(iii) the capability of bad actors penetrating data security measures within Open24,

(iv) the likelihood of bad actors penetrating the Open24 data security measures and the consequences of this materialising for both customers and PTSB,

(v) recent trends and developments of techniques that bad actors may use to penetrate the Open24 security measures and systems,

(vi) the adequacy of PTSB's procedures and systems to mitigate risk of customer data being compromised, and

(vii) PTSB's other legal and regulatory obligations such as the Consumer Protection Code 2012 and Payment Account Regulations 2016.[18]

71. PTSB stated that as a regulated entity, it had an Internal Control Framework ('**ICF**') which set out the structures, frameworks, policies and procedures employed by PTSB to ensure, among other things, safe management of data protection and security.[19] This is governed by its Enterprise Risk Management Framework ('**ERMF**'), which sets out an "*approach to risk identification, assessment, measurement, mitigation, control, monitoring, testing, and reporting across the Three Lines of Defence*."[2021]

72. ERMF, it was noted, is in turn supported by "*a set of frameworks, policies, and procedures (including methodologies and standards) that provide the foundation and structure for PTSB's approach for effectively and efficiently designing, implementing, monitoring, reviewing, and continually improving risk and compliance management across the*

[17] PTSB Operational Risk Management Framework January 2021, p2.
[18] PTSB response to commencement Notice 12 September 2022 p3.
[19] PTSB response to commencement Notice 12 September 2022 p4.
[20] PTSB response to commencement Notice 12 September 2022 p4.
[21] The Three Lines of Defence is a common risk management and internal control framework. The first line owns and manages risk directly. It identifies, assesses and controls risks as part of day-to-day activities. The second line consists of separate risk management, compliance, monitoring and control functions, which provides *inter alia* policies/frameworks and oversight to the first line. The third line consists of an internal audit function which provides independent assurance of the first two lines.

enterprise (including data protection risk)."[22] These risk management processes include activities such as PTSB's Risk and Control Self-Assessment exercise ('**RCSA**'), monitoring risk activities (including data protection risk), and the control testing of those risks.

73. As noted above, PTSB stated that it operates a 'Three Lines of Defence' approach to the assessment and management of risk, including data protection risk. In the First Line of Defence ('**1LOD**'), PTSB stated that an active RCSA was maintained which set out an assessment of Open24's data protection risks and the risk to any data subject, which arise from the team's activities both in terms of likelihood of the risks, and the severity of the impact of the occurrence of those risks. PTSB considered that the RCSA enabled it to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security.[23] In this regard, the risk ratings were assessed using the Group Materiality Matrix[24] and PTSB then implemented technical and organisational measures in Open24 to mitigate identified and inherent risks and the residual risk was also assessed.[25] The 1LOD was also required to escalate and report on any [redacted] Risk Acceptance through the relevant governance process.[26]

74. In its submissions in response to the Inquiry Commencement Notice, the data protection and data subject risks relevant to the Open24 Contact Centre RSCA, along with their risk rating, were outlined by PTSB as follows. First, PTSB stated that the risk of inappropriate disclosure of information to customers or third parties was given an inherent risk of [redacted], the highest risk score within PTSB's risk framework. Second, the risk of inadequate protection of customer data, including customer data transmitted to and/or shared to/from third parties engaged by PTSB, was also given an inherent risk of [redacted]. Finally, the risk of untimely or non-reporting of 'Data Protection Breaches' per PTSB's Data Security Breach Procedures, was given an inherent risk of [redacted] which is the 2nd highest risk score within PTSB's risk framework.[27]

75. However, in its submissions in response to the Issues Paper, PTSB clarified that, at the time of the Breaches, Open24's RSCA had six data protection related risks documented with the

[22] PTSB response to commencement Notice 12 September 2022 p4.
[23] PTSB response to commencement Notice 12 September 2022 p5.
[24] According to which risks were rated as Critical, Significant, Important or Minor.
[25] PTSB response to commencement Notice 12 September 2022 p5.
[26] Permanent TSB Bank, Risk and Control Self-Assessment Process, January 2022, p19.
[27] PTSB response to commencement Notice 12 September 2022 p5.

inherent risks rated as follows: [redacted][28] The relevant extract from the RSCA is set out at Appendix 1 below and the risks identified therein were as follows:

(i) The risk that the Bank does not have the appropriate technical and organisation measures to secure data leading to unauthorised access or disclosure due to human error or inadequate procedures or processes, resulting in potential data breaches, regulatory censure, customer detriment, reputational damage and/or financial loss.

(ii) The risk that the confidentiality, integrity and availability of the Bank's assets, including systems and data, are compromised potentially leading to data breaches, unavailability of systems, inability to access data, unreliable data resulting in negative customer impact, breach of regulatory obligations and financial loss, reputational damage, regulatory censure or sanction.

(iii) The risk that new and/or existing staff are not suitably qualified or trained for their role resulting in regulatory breaches, and / or customer detriment.

(iv) The risk of failure to attract, retain or engage staff leading to insufficient resources to deliver business activity resulting in financial loss, reputational damage, regulatory breaches and/or customer detriment.

(v) The risk of inadequate, incomplete, inaccurate, and lack of adherence to frameworks and policies resulting in failure to consistently achieve and deliver business objectives.

(vi) The risk of external fraud perpetuated on customers/PTSB accounts, banks systems and/or bank staff resulting in breaches of regulatory requirements, regulatory censure, customer detriment, reputational damage and/or financial loss.

76. PTSB submitted that the RSCA "*is robust and effectively considers the data protection risks applicable to customers interacting with the Open24 Contact Centre*".[29] In addition, it was submitted that, in line with the 'Three Lines of Defence' approach to the assessment and management of risk, the "*RSCA is subject to frequent review and challenge by both the [First*

[28] Those risks where then assessed and assigned a residual risk rating (the risk that remained after considering the extent to which controllers or other factors mitigate the risk) as follows: 3 Significant, 1 Important, 2 Minor.
[29] PTSB response to the statement of issues of 16 February 2024, p4.

Line of Defence] and Second Line of Defence, and the maintenance of the Open24 RCSA and its controls means PTSB monitors emerging data protection and data security risks and mitigants within the Open24 Contact Centre."[30]

77. PTSB submitted that its second line of defence ('**2LOD')**, which operated as an independent risk management function, supported and challenged its 1LOD RCSA and aimed to ensure that appropriate technical and organisational data protection and data security measures were in place, and were operating effectively, to manage the risks of customer data being compromised.[31] In addition to developing and maintaining relevant risk frameworks and policies, the 2LOD was required to engage in "[*r]egular reporting to [the] Board and Senior Management*."[32] Similarly, the 2LOD was required to monitor risk and challenge "*the sufficiency of business-unit monitoring activities*", as necessary. The 2LOD was also required to escalate issues "*if risk management concerns [we]re not adequately addressed by the [1LOD]*".[33]

78. PTSB further stated that its third Line of defence ('**3LOD')**, which comprised the Group Internal Audit Function ('**GIA**'), also formed part of this risk assessment and provides independent reasonable assurance to PTSB's Board of Directors regarding the effective operation of the governance, risk management and control processes established and maintained by the First and Second Lines of Defence.[34]

79. In assessing the relevant risks, the DPC notes that PTSB processed a vast quantity of personal data in the Open24 platform in respect of a large number of data subjects. The key elements of the service provided by Open24 include enabling customers to access their account balance, get information about their transactions, set up or view standing orders, carry out cheque searches, transfer funds and make payments, pay bills, request account statements, top-up mobile phones, register and view other PTSB accounts, view recent credit card transactions, customise current account transaction history on screen, and show policy details. The potential risks associated with unauthorised persons being able to access and use another user's account include identity theft, fraud and financial loss.[35]

[30] PTSB response to the statement of issues of 16 February 2024, p4.
[31] PTSB response to commencement Notice 12 September 2022, p5-6.
[32] Permanent TSB Group Regulatory Compliance Framework, p20.
[33] Permanent Operational Risk Management Framework, p15.
[34] PTSB response to the statement of issues of 16 February 2024, p18.
[35] See Recital 75 GDPR.

80. The DPC notes that PTSB had itself considered that a number of critical risks arose in the context of its Open24 Contact Centre, including (i) that appropriate technical and organisational measures were not in place to secure data, leading to unauthorised access or disclosure due to human error or inadequate procedures or processes; (ii) the risk that new and/or existing staff are not suitably qualified or trained for their role resulting in regulatory breaches and (iii) the risk of external fraud perpetuated on customers/PTSB accounts, banks systems and/or bank staff.[36] Additional risks, given a rating of [redacted] included "*the risk of inadequate, incomplete, inaccurate, and lack of adherence to frameworks and policies*".

81. In the circumstances, the DPC considers that, on an objective assessment, PTSB's processing of personal data via its Open24 Contact Centre presented a variety of risks that were of high likelihood, including unauthorised access, alteration or disclosure of customer data, requiring proper evaluation and management. The DPC makes this finding in light of the sensitivity of personal data processed which included financial data and therefore poses a target for bad actors. The quantity of personal data processed, the number of users and the purposes of that processing together posed a significant risk in terms of likelihood. The high volume of calls received in the Open24 Contact Centre and the external fraud environment also led to a high likelihood of those risks arising. This underscores the need for appropriate measures to mitigate such high risk.

82. The severity of the risks to the rights and freedoms of data subjects was also high. The DPC makes this finding in light of nature of the personal data processed. This processing entailed a significant amount of personal and financial data. In the event of unauthorised access by bad actors, data subject identity, contact details, economic or financial data could be misused to the detriment of data subjects, as was case in the Breaches. Therefore, having regard to this high risk, it was incumbent on PTSB to implement appropriate technical and organisational measures as required by Article 32 GDPR.

ii. Measures Implemented by PTSB and Appropriateness of those Measures

83. The principle of integrity and confidentiality set out in Article 5(1)(f) GDPR requires that the controller ensures appropriate security of personal data when processing using appropriate technical or organisational measures. Article 32(1) GDPR requires that the controller shall assess the risk to data subjects of the particular processing and shall implement appropriate

[36] PTSB response to the statement of issues of 16 February 2024, Appendix 3.

technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the factors listed in that Article.

84. PTSB's submissions outlined the technical and organisational measures that it had in place at the time of the Breaches to ensure the ongoing confidentiality and integrity of personal data processing in the Open24 Contact Centre.

(i) Technical measures

85. In addition to the policies and procedures noted below, PTSB described specific technical measures that it stated were in place at the time of the Breaches, including:

(i) Strong Customer Authentication ('**SCA'**) – PTSB implemented SCA, which required multi-factor authentication for online transactions and push notifications on completion of certain actions. In this regard, when a PTSB customer made an online transaction, a push notification was received through the Open24 app or via SMS for the customer to verify the transaction. As an additional control, a push notification was sent to the customer's registered mobile phone number when completing certain actions through Open24 telephone and online services. Examples of these included the adding of a payee on a bill payment or confirming an online transaction.[37]

(ii) Fraud Monitoring System ('**ARIC**') – PTSB's fraud monitoring system identified certain changes to customer profiles and transactions conducted through the Open24 Contact Centre. [redacted].[38]

86. While PTSB did have technical measures in place, these technical measures did not include additional controls to prevent foreseeable human error and respond to predictable attacks likely to be faced by the Open24 Contact Centre. In relation to the Breaches, PTSB staff/agents manually altered customer account information without any form of

[37] PTSB response to commencement Notice 12 September 2022 p6-7.
[38] PTSB response to commencement Notice 12 September 2022 p15.

mandatory backend validation measures or prompts to the staff member to use the necessary security protocols. Staff/agents were in a position to alter important account details, such the phone number used for two factor authentication, or allow bad actors to re-register and take over accounts, while repeatedly failing to pass the relevant security protocol. Where PTSB staff /agents are in a position to alter customers' personal data with the possible serious knock-on effect of unauthorised access to the customers' accounts, there is an obligation on PTSB to regularly assess and evaluate the effectiveness of measures in place to ensure that they are appropriate and responsive to the level of risk present. Furthermore, there must be an ongoing and verifiable oversight of how the staff/agents give effect to the controller's policies and procedures and technical measures should be put in place to ensure that the relevant security protocols are followed before significant actions are taken in relation to an account.

87. The lack of appropriate technical safeguards was significant and was exploited by the fraudulent actors in the Breaches. There were a number of technical measures that PTSB could have implemented prior to the breaches to provide a level of security appropriate to the risk, including enforced backend validation of login attempts to reduce agent subjectivity and error, logging of unsuccessful attempts at account access via the Open24 Contact Centre, warnings that a number of unsuccessful attempts had been made to access the account in the previous days or weeks to access or change account information, or prompts to ensure that correct security procedures are followed by staff/agents prior to accessing an account or changing account details via the Open24 Contact Centre.

88. An appropriate level of security includes technical measures that have, amongst other things, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. While PTSB had technical measures in place at the time of the Breaches, the lack of a control on foreseeable human error meant that the level of technical security measures was not sufficient to ensure the safety and confidentiality of the data being processed by PTSB in the context of the Open24 Contact Centre, in light of the high risks inherent in that processing. Therefore, the DPC considers that the technical security measures in place at the time of the Breaches did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

(ii) Organisational Measures

Data Protection Governance

89. PTSB outlined the data protection policies and procedures it had in place at the time of the Breaches including:

(i) Data Protection Policy which was reviewed annually and/or following any significant market, regulatory or business developments impacting it;[39]

(ii) Information Security Policy, which set out the requirements for PTSB (and third parties with whom PTSB engages) to manage its information and information technology systems in a manner that appropriately protects the security of the information stored and processed in those systems such as Open24.[40]

(iii) Fraud Prevention Policy, which governed all staff and business units, and according to which, all new products or changes to existing products require consideration from a fraud risk perspective, engagement with the Financial Crime & Loss Prevention Unit for advice, and where required, a complete Fraud Risk Assessment.[41]

(iv) Digital and Direct Security Manual which provided information on all relevant security procedures for PTSB's Digital & Direct Service team, including the "security journeys" for incoming calls. [redacted][42]

(v) Data Management Policy which was derived from the best practices of the Data Management Association's Data Management Framework. Other policies, such as the Records Management and Data Quality policies were subordinated to the Data Management Policy.[43]

[39] PTSB response to commencement Notice 12 September 2022 p12-13.
[40] PTSB response to commencement Notice 12 September 2022 p14.
[41] PTSB response to commencement Notice 12 September 2022 p16.
[42] PTSB response to commencement Notice 12 September 2022 p32-33.
[43] PTSB response to commencement Notice 12 September 2022 p13.

(vi) Data Security Breach Policy which set out the responsibilities for all employees in relation to the identification and reporting of breaches of personal data to the 2LOD.[44]

90. PTSB's Data Protection Officer ('**DPO'**) and data protection team which advised, monitored and reported on compliance with data protection obligations as part of the 2LOD.[45]

91. PTSB further stated that the design of PTSB's risk management process, in line with European Banking Authority Guidelines, was underpinned by traditional risk management objectives and principles. Risks were identified, assessed, measured, monitored and reported on by business units and functions that incur risks as a result of their frontline commercial and operational activities. The 2LOD, it was submitted, ensured that all risks were identified, assessed, measured, monitored, managed and properly reported on by the relevant units in PTSB.[46]

92. The DPC is satisfied that PTSB had a range of important Data Protection Governance policies and procedures in place to provide for the integrity and security of customers' personal data. However, these policies and procedures were deficient because there was no procedure in place to notify a manager or place any alert on an account following unsuccessful attempts to access or change account details by phone. As a result, bad actors in possession of certain information were able to repeatedly test the security procedures without consequence, as evidenced by the Breaches. This further allowed bad actors to seek to extract information from numerous agents in an effort to obtain the full range of security questions associated with an account. For example, in the cases of BN-22-5-469 and BN-22-5-49, PTSB identified that the bad actor made 51 calls to the Open24 Contact Centre.

93. Furthermore, policies and procedures cannot be effective where they are not adhered to by staff and the Breaches provide evidence of significant non-adherence to some of those policies. In the cases of the Breaches leading to financial loss (BN-22-5-469 and BN-22-5-497) the DPC notes that the root cause was identified as *"(i) agents not fully following the security procedure and (ii) agents not being aware of the additional procedural requirements when dealing with change of contact number requests for customers with a connection and/or address in* [redacted].[47] The Breaches illustrate numerous instances

[44] PTSB Data Security Breach Policy, May 2018.
[45] PTSB response to commencement Notice 12 September 2022 p12.
[46] PTSB response to commencement Notice 12 September 2022 p11.
[47] PTSB response to commencement Notice 12 September 2022 p19.

of staff/agents not following appropriate security procedures, including numerous instances of different staff/agents not following appropriate procedures in the case of the same data breach. For example, in the context of BN-22-5-497, the correct security procedures were not followed on at least five calls with five separate agents. Similarly, in the context of BN-22-5-469, appropriate procedures were not followed on at least three separate occasions leading to the occurrence of repeated personal data breaches.

94. Given the high risk to the rights and freedoms of PTSB customers, and given the sensitivity of the personal data processed by PTSB, PTSB ought to have implemented appropriate procedures to ensure that its data protection policies and risk management policies were followed by staff/agents. As detailed further in the DPC's consideration of the training and organisational measures below, the DPC considers that the checks and enforcement measures in place, at the time of the Breaches, were inadequate to ensure this was the case. In particular, the level of initial training and testing of staff on the relevant security procedures was insufficient, an issue which was aggravated by the various security journeys in place and the lack of appropriate measures to account for when they were repeatedly not followed.[48] Furthermore, the level of monitoring fell below the required standard in light of the high risks to data subjects.

Training and Awareness

95. PTSB stated that team members in its Digital and Direct team, which houses the Open24 Contact Centre, were "*required to complete on-going Data Protection Training and Development Courses which have been developed by PTSB's Data Protection Team*". Completion was monitored by PTSB's Human Resources team.[49]

96. PTSB also stated that the "*Open24 contact centre provides detailed training to members of staff handling calls on behalf of PTSB as part on the Onboarding Process*".[50] This training was two weeks long - now three weeks - and all staff were required to pass one simulated call prior to handling calls from customers on the Open24 system.[51]

[48] Security Journeys are described by PTSB as "internal security procedures and controls in place for dealing with incoming calls" and are discussed in more detail at paragraph 105.
[49] PTSB response to commencement Notice 12 September 2022 p9-10.
[50] PTSB response to commencement Notice 12 September 2022 p9.
[51] PTSB response to Statement of Issues 24 February 2024 p6.

97. PTSB also submitted that the data protection team release awareness notices to all PTSB employees, including those in the Open24 Contact Centre. PTSB stated that "*data security and data protection risk*" was a key component of these trainings. PTSB provided details of the training courses, which have been given since 7 September 2022, and which included training on account registration, security processes, and the changing of personal details.[52]

98. PTSB stated that staff, including those in the Open24 Contact Centre, are required to complete annual ongoing mandatory Learning and Development courses on specific subject matters. PTSB gave details of courses including Operational and IT Risk Awareness, Business Continuity Management and Conduct Risk which were undertaken prior to the Breaches in 2022. Training courses that have taken place subsequent to the Breaches have included Fraud Awareness, Cyber Security and Data Protection.[53] In the Data Protection course launched in June 2023, specific reference was made to the Breaches.[54]

99. In general, data protection training needs to be frequent and regular to a degree that is appropriate to the risk of the processing having regard to the activities being carried out. The sensitivity of the data processed by PTSB, the detailed nature of its Open24 platform which users use to access their financial data means that training should have been provided to staff frequently and in sufficient detail in order to reduce the likelihood of fraud leading to loss of confidentiality of personal data, as occurred in the Breaches.

100. Training should also be informed by the risks arising from the processing activities, as outlined in risk assessments, and should be regularly updated as the risk landscape changes. PTSB had previously identified phone calls from South African numbers as a contributing factor in relation to the unauthorised disclosure of account information in certain cases. This issue was originally identified by PTSB as early as 2020 and accordingly it put additional steps in its staff onboarding programme. However, these steps were removed before the Breaches occurred. The steps have subsequently been reintegrated into the onboarding training programme.[55]

101. The DPC finds that the level of training provided to new staff prior to the Breaches, including only one simulated call, was insufficient in light of the serious risks involved in the processing, coupled with the ability of call agents to manually alter data without security protocols being followed. This is particularly the case where the processing had a high risk

[52] PTSB response to commencement Notice 12 September 2022 p35.
[53] PTSB response to commencement Notice 12 September 2022 p35-37.
[54] PTSB response to Statement of Issues 24 February 2024 p14.
[55] PTSB response to commencement Notice 12 September 2022 p41.

to the rights and freedoms of natural persons including identity theft, fraud or financial loss as highlighted by Recital 75 GDPR.[56] The DPC additionally notes that an internal audit conducted by PTSB following the Breaches identified issues with initial staff training and concluded that the structure of this training was "*not sufficient given the evolving nature of Customer Contact Centre processes and systems*".[57] This is particularly relevant in the context of the Breaches as the events that are the subject of this Inquiry involved staff who were new to the Bank at the time and had thus recently completed their initial training.[58]

102. Considering the importance of maintaining the security of customers' accounts and the high risks to the customer arising as a result of unauthorised disclosure, PTSB ought to have implemented more comprehensive training and evaluation processes to ensure that the likelihood of agent error, either through unfamiliarity with PTSB procedures, social engineering methods employed by bad actors or human error in relation to data entry, was minimised appropriately. In particular, the nature of the personal data processed through the Open24 Contact Centre increased the likelihood of bad actors carrying out targeted attacks in order to carry out fraud. As a result, more rigorous initial training and testing with simulated calls to ensure adherence to the relevant security procedures ought to have been put in place.

Additional organisational measures

103. PTSB outlined that it had a range of additional organisational measures relating to security, the most relevant of which are detailed below.

Security Journeys

104. The Open24 Contact Centre allowed a customer to securely identify themselves outside of the SCA via either the Branch Security (Standard) process or the Enhanced Security process. PTSB stated that these alternative processes could apply in situations including where

[56] Recital 75 states: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;…"
[57] PTSB response to commencement Notice 12 September 2022, Appendix 14.
[58] PTSB response to Statement of Issues 24 February 2024 p13.

customers lacked the capability or capacity to operate in the on-line channel or were unable to attend physically.[59]

- Branch Security (Standard) process - [redacted] This process did not allow the agent to give out any additional information on the account and was only used when customers required very basic services, such as the confirmation of an expected lodgement.[60]
- The Enhanced Security process – [redacted].[61]

105. PTSB also provided details of the four "security journeys" available to agents for incoming calls at the time of the incidents. In Security Journey number 1, callers were verified by [redacted] No further security questions were required as PTSB considered that this was sufficient for the customer to demonstrate that they were a registered customer.

106. Security Journey number 2 applied to callers who were registering for Open24 access and required [redacted]

107. Security Journey number 3 applied to callers who were not registered for Open24 [redacted] No financial transactions could be instructed under this security journey.

108. Security Journey number 4, "Enhanced Security", was used in situations where a customer was requesting to complete a change in their personal details and/or setting up a

[59] PTSB response to commencement Notice 12 September 2022 p7-8.
[60] PTSB response to commencement Notice 12 September 2022 p7.
[61] PTSB response to commencement Notice 12 September 2022 p7.

payee/standing order. The customer was asked to either [redacted]

109. The DPC notes that following the Breaches, PTSB limited use of the third security journey (standard/ branch security) to customers who completed either the Enhanced Security process or were registered for Open24 access. The DPC finds that this was an inadequate security measure in light of the risk in the circumstances and considers that the use of such minimal purely knowledge-based authentication should be avoided. The ease with which an attacker can discover the answers to many static knowledge-based questions, and the relatively small number of possible choices for responding to many of them, results in this method having a high risk of successful use by an attacker. This was aggravated in this case by PTSB staff/agents accepting only partial answers with no technical safeguards in place to prevent this. Whilst static knowledge-based questions may provide an additional security layer in the absence of more secure measures, in certain limited circumstances, they should not be relied upon as the sole mechanism to identify a user. This is all the more the case when the processing is high risk in nature and has potentially severe consequences for data subjects, including financial loss.

110. As evidenced by the Breaches, bad actors in possession of account holder information such as name, address, email address, mobile phone numbers etc. can use such information to bypass weak security requirements, in order to obtain more information, which can be used to further an attack. In addition, in the context of the Open24 Contact Centre, as detailed above, bad actors were able to repeatedly test the security procedures as there was no rate limit when incorrect answers were provided, and repeated failed authentication attempts via the Open24 Contact Centre were not logged or notified to the account holder, which heightened the risk flowing from such inadequate procedures. It also appears that the use of more minimal security measures for certain actions may also have caused confusion to PTSB agents, leading to potential use in scenarios where it was identified as not being appropriate,[62] with no technical measures in place to prevent this. Ultimately, the Open24 Contact Centre provided a less secure backdoor in to otherwise secure accounts and presented a clear and predictable target for attackers.

[62] PTSB response to commencement Notice 12 September 2022, Appendix 15 p 5.

Monitoring of Calls/Adherence to Security Procedures

111. In addition to the above, PTSB carried out call quality assurance on calls handled by staff/agents, including the following:

- The Retail Channel Assurance Team ('**RCAT**') monitoring compliance with the Digital and Direct Security Manual and more particularly the Scripting & Adherence contained in the Digital & Direct Security Manual, and the Open24 Service Scripting. The frequency of checks to monitor compliance was determined on a risk-based approach with calls pertaining to change of personal information to be deemed to be high risk. Such calls were thus regularly monitored by the RCAT. In the case of a change of a mobile phone number, 25% of these calls were monitored by the RCAT for a data quality check (i.e. to confirm that the number was transcribed correctly, as per customer instruction). One call out of this 25% of calls was reviewed in full daily, to monitor compliance including the adequacy of the security check completed. If non-compliance was identified, the RCAT escalated the matter to team leader level in the Open24 Contact Centre.[63]

- Call monitoring quality assurance was completed on between 2 – 5 calls per agent per month, on a risk-based approach. Quality assurance was also provided by RCAT with quality checks on the sample of calls taken by PTSB agents in the Open24 Contact Centre each month using a pre-determined 'Score Card' of standards. The monitoring aimed to evaluate the area of agent calls with customers "*including the adequacy of the security check completed to identify that the agent is in fact speaking with the customer; overall quality; customer interaction standards; procedures including the Digital & Direct Security Manual; the Open24 Service Script; relevant legislation including the Act, the GDPR and the Consumer Protection Code 2012 relating to security and telephone contact provisions; the actions taken on the call*".[64]

- The RCAT evaluated the percentage of administrative actions completed by PTSB agents in the Open24 Contact Centre on an information technology system. These checks were selected from an automated report which was sent from an information technology system to the RCAT each day. The RCAT also collated data and provided a

[63] PTSB response to commencement Notice 12 September 2022 p8.
[64] PTSB response to commencement Notice 12 September 2022 p38.

monthly analysis trend report to highlight risks, including data protection risks, and support continuous training and development of staff.

- Any specific quality assurance findings were notified to agents on the same day upon identification and issues and trends identified as part of the quality assurance processes were shared and discussed with Open24 management to action.

- On a semi-annual basis all Open24 procedures were reviewed by the management team to ensure that the procedures contained correct information and security processes and were compliant with applicable regulations including, but not limited to the Consumer Protection Code 2012 and the Data Protection Act 2018.[65]

112. While there were follow-ups on the part of PTSB with regard to breaches caused by staff not following policies and procedures, the DPC considers that the checks and enforcement measures put in place by PTSB at the time of the Breaches were inadequate. Creating policies and procedures is essential to implementing an appropriate level of security. However, policies and procedures alone are not sufficient to mitigate the risk to data subjects. Where staff handle phone calls pertaining to customer financial information, there is an obligation on a controller to regularly assess and evaluate the effectiveness of measures in place and therefore, there must be an ongoing and verifiable oversight of how staff members give effect to the controller's policies and procedures. This obligation was heightened where there is evidence to suggest that PTSB was previously aware of possible security issues relating to calls originating from [redacted] PTSB stated that it had experience of post being intercepted in [redacted] and previously implemented an "additional steps" guide to be used prior to inputting a [redacted] mobile telephone number on the PTSB customer database. The DPC accepts that it may not have been commercially feasible to monitor all calls pertaining to the changing of a mobile telephone number on a customer file or all calls originating from a [redacted] mobile phone number. However, in circumstances where these two risk factors overlapped, this should have alerted PTSB to the potential risk of unauthorised access and alteration of personal data on the customer account.

113. The DPC has had regard to PTSB's monthly call monitoring, whereby on average between two and five calls per agent per month were monitored and that any issues were notified to agents on the same day. PTSB also stated that it considers calls where a change of

[65] PTSB response to commencement Notice 12 September 2022 p6-7.

personal information is requested, [redacted] to be high risk and in those instances "*25% of calls are monitored by the Retail Channel Assurance Team*". However, as noted above, only one call out of this 25% was reviewed in full daily for all aspects of regular call monitoring including the adequacy of the security completed. The DPC finds that the level of monitoring of adherence to security procedures was not appropriate to the high risk, particularly in light of the level of initial training and testing and lack of technical safeguards described above. In light of the weaknesses in those areas identified above, and the high risk of the processing, more stringent monitoring ought to have been implemented in order to determine how security procedures were being implemented in practice. The confluence of factors led to a situation where initial training and testing of agents was insufficient, there was an absence of sufficiently robust technical safeguards to combat entirely predictable security lapses by those agents, and there was an insufficient level of monitoring meaning that PTSB did not have a clear picture of how its security procedures were in fact being implemented in practice in the Open24 Contact Centre.

114. The Breaches provide clear evidence of significant non-adherence to security procedures by PTSB staff/agents when faced with a motivated attacker. For example, as detailed above, in the context of BN-22-5-497, the correct security procedures were not followed on at least five calls with five separate agents. Similarly, in the context of BN-22-5-469, appropriate procedures were not followed on at least three separate occasions leading to the occurrence of repeated personal data breaches. From an overview of the organisational measures employed by PTSB, there were several areas that posed a risk of personal data breaches including the different forms of customer secure identification which could lead to unauthorised access to account information from malicious actors. Considering the importance of maintaining the security of customers' accounts and the high risks to the customer arising as a result of accounts being compromised, PTSB ought to have implemented more robust monitoring measures to ensure its policies and procedures were being implemented correctly and that it was enabled to promptly identify when they were not.

115. For the above reasons, the DPC therefore finds that PTSB infringed Article 5(1)(f) and Article 32(1) GDPR.

b) Issue 2: Article 33 GDPR

i) The Obligation to Notify Without Delay

116. Article 33 sets out the requirements in respect of notification by a controller to the supervisory authority of a personal data breach. Article 33(1) of the GDPR provides:

> "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*."

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

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

118. Article 33(1) requires that notifications must occur 'without undue delay.' This must be assessed by reference to when PTSB became aware of the personal data breach. In its 'Guidelines 9/2022 on Personal Data Breach Notification under GDPR' (the '**Breach Notification Guidelines**') the European Data Protection Board ('**EDPB**') addressed the meaning of the term 'undue delay' in the related context of the requirement to communicate a breach to affected individuals under Article 34 GDPR:

> "*The GDPR states that communication of a breach to individuals should be made 'without undue delay,' which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves*."[66]

[66] Breach Notification Guidelines p11.

119. The Breach Notification Guidelines further provide that:

> "[A] *controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. However…the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. <u>This puts an obligation on the controller to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action</u>*.[67]" (Emphasis added)

120. The Breach Notification Guidelines go on to consider cases where there is uncertainty as to whether a personal data breach has occurred:

> "*In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.*
>
> *[…]*
>
> *After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.*

[67] Breach Notification Guidelines p11.

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach.

[…]

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases."

121. There is also provision for phased notification, as set out in Article 33(4) GDPR, which provides that *"[w]here, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay*."

122. With regard to the requirement to put in place appropriate measures to establish whether a data breach has occurred, Recital 87 GDPR states:

"*It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation*."

123. The Breach Notification Guidelines state that:

"[T]*he GDPR requires both controllers and processors to have in place appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Also the GDPR requires all appropriate technological protection and organizational measures to be in place to establish*

immediately whether a breach has taken place, which then determines whether the notification obligation is engaged. Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner."[68]

124. Article 33(1) GDPR cannot be viewed in isolation and must be understood within the context of the broader obligations on controllers under the GDPR, such as the obligation of accountability under Article 5(2) and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24, 25 and, in particular, Article 32 GDPR. Regard must be had to these obligations in determining the point in time in which the controller should have been 'aware' of the existence of a personal data breach for the purposes of Article 33 GDPR.

125. In considering whether PTSB complied with its obligation to notify a personal data breach under Article 33(1), therefore, the DPC has considered the objectives underlying this obligation and the broader context in which this obligation arises.

ii) The Breach Notifications

126. By way of brief recap, initial contact with the DPC was made by a PTSB member of staff on 26 May 2022 in respect of BN-22-5-459 stating that a personal data breach had occurred at PTSB on 8 April 2022. PTSB initially indicated that it became aware of the breach via data subject notification on 8 April 2022. However, it transpired that the Data Protection Team had not been informed of the potential data breach at that time and only became aware of the matter over the course of an investigation into a formal complaint lodged by the customer.

127. PTSB subsequently stated in its submissions that, notwithstanding that the initial breach notification form stated that PTSB became aware of the personal data breach aspects on 8 April 2022, this was in fact the date on which PTSB became aware of the fraud aspect of the incident when contacted by the customer.[69] The customer contacted PTSB again on 16 April, whereby he notified PTSB that he was having difficulty completing transactions from a different, joint-owner current account held with PTSB. Upon further investigation, PTSB determined that the phone number on file had been updated by a malicious actor, on 8

[68] Breach Notification Guidelines, p6.
[69] PTSB response to commencement Notice 12 September 2022 p27.

April 2022, and that this incorrect number remained on the account until 16 April. In correspondence to the data subject, dated 1 July 2022, PTSB confirmed that following the call from the data subject on 16 April, "*it was at this stage following a full investigation that the extent of the breach and compromise became clear to us*." PTSB thereafter removed the fraudulent phone number from the bank systems, cancelled the PAN and debit cards and placed transaction holds on the accounts. The fraud team further contacted the data subject by phone on 20 April to advise of the closure of the data subject's account on the same date. The Data Protection Team were not informed.

128. PTSB submitted that it was only following the receipt of the monthly complaint listings from its Customer Resolution Centre,[70] on 6 May 2022, that the data protection team ultimately initiated an investigation into the matter (on 19 May 2022) to determine whether a data breach had in fact occurred. PTSB stated that, on 20 May 2022 (at 12:17), the data protection team determined with a reasonable degree of certainty that a personal data breach had occurred requiring notification to the DPC and the data subject.[71] Thereafter, on 26 May 2022 (at 16:52), the data protection team submitted a personal data breach notification to the DPC in relation to incident.

129. In respect of the remainder of the Breaches, initial contact was made with the DPC on 27 May 2022 via Breach Notification forms BN-22-5-469 and BN-22-5-497 stating that personal data breaches had occurred at PTSB respectively on 20 April and 6 May 2022. PTSB initially indicated that it became aware of these breaches via data subject notification on 3 May and 9 May 2022 respectively. However, the Data Protection Team had not been informed and only became aware of these breaches over the course of a fraud investigation.

130. PTSB subsequently stated in its submissions that the above date of data subject notification in BN-22-5-497 was in fact the date that PTSB's "*fraud team became aware of the fraudulent attack committed by the bad actor on PTSB and its customer*".[72] Following a full review of all of the call transcripts involving the bad actor by the digital and direct risk team, the Data Protection Team was subsequently engaged "*on 24 May 2022 (at 13:46) and*

[70] In relation to customer complaints, where the CRC receives a complaint that CRC suspect may be a data breach CRC must engage with the data protection team as per PTSB's Data Security Breach Procedure and the procedure set out above must be followed. Additionally, the data protection team engage with CRC on a monthly basis to obtain a list of complaints which indicate that there is a data protection related grievance on PTSB's complaint management system. This list is reviewed and compared to the data protection team's records in order to ensure that all data security breach incidents have been referred to the data protection team for review.
[71] PTSB response to commencement Notice 12 September 2022 p27.
[72] PTSB response to commencement Notice 12 September 2022 p22.

determined with a reasonable degree of certainty that a personal data breach had occurred requiring notification to the DPC and the data subject."[73] A risk event was also logged by the Digital & Direct Risk Team on 24 May 2022 (at 16:38) on the Governance, Risk and Compliance ('**GRC**') system in order to flag a potential personal data breach. The Data Protection Team then carried out an assessment of the incident and, on 27 May 2022 (17:50), the Data Protection Team submitted a personal data breach notification to the DPC.[74]

131. Similarly, in relation to BN-22-5-469, PTSB stated that *"[n]otwithstanding that the initial breach notification form from PTSB to the DPC in relation to BN-22-5-469 (R2217) stated that PTSB became aware of the personal data breach on 3 May 2022, this is in fact the date on which PTSB became aware of the fraud aspect of the incident. PTSB had a reasonable degree of certainty that a personal data breach occurred on 23 May 2022*."[75] In this instance, a risk event was logged by the Digital & Direct Risk Team on 23 May 2022 (at 11:05) on the GRC system in order to flag a potential personal data breach. The Data Protection Team carried out an assessment of the incident and issued an email to the Digital & Direct Risk Team on 23 May 2022 (at 12:54) confirming the incident was deemed a reportable event. PTSB subsequently submitted a personal data breach notification to the DPC on 27 May 2022 (at 16:07).

132. The DPC considers that there is no justification for the considerable length of time taken to determine that a data breach had occurred in each of the above three instances. The fact that financial fraud had been committed in two cases, and that customer account contact details had been altered in all three instances, shortly before the customers advised PTSB of the issues, should have immediately alerted PTSB to the probability that personal data breaches may have occurred. In light of this, and the potentially severe financial consequences for the affected data subjects, it was incumbent on PTSB to take prompt action to investigate the incidents to determine whether personal data had indeed been breached, and if so, to take remedial action and notify the DPC if required.

133. The DPC has also had regard to PTSB's Data Security Breach Procedure which clearly set out PTSB's obligations to report on data breaches. The Procedure noted that PTSB was "*required to report personal data breaches to the Data Protection Commission (DPC) within*

[73] PTSB response to commencement Notice 12 September 2022 p28.
[74] PTSB response to commencement Notice 12 September 2022 p28.
[75] PTSB response to commencement Notice 12 September 2022 p28.

72 hours", which is the requirement under Article 33(1) GDPR.[76] This referred to all instances of loss of control of personal data, regardless of the number of customers impacted. The Breach Procedure also provided that in the event of doubt as to whether a breach had occurred, that the staff member "*should contact the Data Protection team by email… or telephone a member of the team*."[77]

134. The DPC considers that this is an adequate policy in the circumstances and that if implemented properly should allow PTSB to meet its reporting obligations, provided the data protection team ensures that a personal data breach notification issues to the DPC within the prescribed 72-hour period. In particular, a cautious approach is warranted whereby any issues potentially relating to any loss of control of personal data will be reported to the data protection team. This is especially important in light of the sensitive nature of the financial data involved. However, in the case of the Breaches, they were not brought to the attention of the data protection team in a timely manner, even when the instances of fraud should have alerted any staff member involved of the necessity to report the incidents.

135. In its submissions in response to the Inquiry Commencement Letter, in referring to the delay in notification of the Breaches, PTSB advised that *"[a]s soon as the Digital & Direct Risk Team had carried out their review of the accounts, listened to the relevant call transcripts involving the bad actors and identified the occurrence of a potential personal data breach, the Data Protection Team was made aware*."[78] However, in light of the requirement for notification to the DPC within 72 hours of having a reasonable degree of certainty that a breach had occurred, and PTSB's own policy that potential incidents should be brought to the attention of the Data Protection Team to make such a determination, it is the view of the DPC that the Data Protection Team were not notified in a timely manner, and in line with PTSB's policy, in each of the Breaches.

136. The DPC takes note that PTSB subsequently took steps to prevent such a recurrence. For example, the PTSB fraud team issued instructions on data security and breach reporting procedural requirements to all staff on 12 July 2022. An amended response strategy was also put in place to respond to urgent requests for investigation of potential data breaches that require review and escalation to assist fraud investigations.[79] Nonetheless, the

[76] PTSB Data Security Breach Policy, May 2018 p1.
[77] PTSB Data Security Breach Policy, May 2018 p1.
[78] PTSB response to commencement Notice 12 September 2022 p27.
[79] PTSB response to commencement Notice 12 September 2022 p30.

appropriate procedure was not followed in the context of the Breaches, leading to a significant delay in notification.

137. In referring to the additional delay in notification, once the Data Protection Team had eventually been notified, PTSB also stated that:

> *"*[T]*he Data Protection Team wanted to ensure that all relevant information, facts and documents relating to the incident were reviewed in order to make a notification to the DPC. This involved numerous engagements with the Digital & Direct Risk Team and the Fraud Team."*[80]

138. While PTSB may not have been fully aware of all of the elements of the Breaches within 72 hours of becoming aware of each breach, it would have been a more correct course of action to alert the DPC to the possibility of a data breach without undue delay, supplementing this with any subsequent relevant information that came to light. Article 33(4) GDPR explicitly recognises the possibility of the controller providing breach information in phases. This is especially important in circumstances where there was a significant delay in PTSB determining that data breaches may have occurred, following the notification from each of its customers, and in circumstances where its Data Protection Team had not been notified in a timely manner, as envisaged by its own internal Data Security Breach Procedure. In the circumstances, the DPC is satisfied that PTSB did not proceed in a sufficiently timely manner to determine whether personal data breaches had occurred upon being notified of the incidents.

139. Controllers are not under an obligation to notify the DPC if a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, the DPC is satisfied that the Breaches did result in such a risk, as evidenced by the financial fraud perpetrated and the risk of further financial fraud and loss of data subject control over their accounts. In assessing risk, regard must also be had, objectively, to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It is also appropriate to have regard as to whether the personal data has come into the possession of individuals whose intentions are unknown or possibly malicious. In the circumstances, the DPC is satisfied that the Breaches resulted in a risk to the rights and freedoms of data subjects, including, but

[80] PTSB response to commencement Notice 12 September 2022 p27.

not limited to, financial loss and loss of control over the data subjects' accounts. Therefore, PTSB was obliged to notify the DPC of the Breaches without undue delay.

140. In light of the above, the findings of the DPC in relation each of the Breaches are summarised below:

(i) In BN-22-5-459, PTSB claimed that it became aware of possible fraud on 8 April 2022 and only determined that a personal data breach had occurred on 20 May 2022. An official breach notification was submitted to the DPC on 26 May 2022, which is 48 days after PTSB first became aware of the fraud incident and 6 days after its Data Protection Team was notified of the incident. The incident was not brought to the attention of the Data Protection Team prior to this date, despite calls from the data subject on 8 April 2022 and 16 April 2022, following which the existence of the breach became apparent. In correspondence to the data subject, dated 1 July 2022, PTSB confirmed that following the call from the data subject on 16 April, "*it was at this stage following a full investigation that the extent of the breach and compromise became clear to us.*" PTSB thereafter removed the "*fraudulent phone number*" from the bank systems, cancelled the PAN and debit cards and placed transaction holds on the accounts. The fraud team further contacted the data subject by phone on 20 April to advise of the closure of the data subject's account on the same date. The Data Protection Team still had not been informed at this point, by which PTSB ought to have been aware of the breach. The data subject later made a complaint, which was only brought to the attention of the Data Protection Team by way of its receipt of monthly complaint listings from the CRC on 6 May 2022. There was a subsequent delay in the Data Protection Team investigating the incident (which occurred on 19 May 2022) and determining that a breach had occurred (which occurred 20 May 2022). There was then an additional delay in the breach notification being submitted to the DPC, on 26 May 2022. The DPC is therefore satisfied that PTSB did not meet its obligations to determine whether a breach had occurred in a timely manner and notify the DPC of the data breach without undue delay and where feasible not later than 72 hours of having become aware of it (i.e. from 16 April 2022 at the latest).

(ii) In BN-22-5-469, PTSB claimed that it became aware of possible fraud on 3 May 2022 and only determined that a personal data breach had occurred on 23 May 2022. The official breach notification was submitted to the DPC by PTSB on 27 May 2022, which is 23 days after it became aware of the fraud incident and 4 days after its Data Protection Team had fully determined that a data breach had occurred,

following an internal delay in notification. The fraud team had first conducted a detailed investigation, including a call listening exercise, which took place from 19-24 May, and it appears that it was in the course of this fraud investigation that it was established that a data breach had occurred. The DPC is therefore satisfied that PTSB did not meet its obligations to determine whether a breach had occurred in a timely manner and notify the DPC of the data breach without undue delay and where feasible not later than 72 hours of having become aware of it.

(iii) In BN-22-5-497, PTSB claimed that it became aware of possible fraud on 9 May 2022 and only determined that a personal data breach had occurred on 26 May 2022. The official breach notification was submitted to the DPC by PTSB on 27 May 2022 (at 17:50), which is 18 days after it became aware of the incident and 1 day after PTSB asserts that its Data Protection Team determined that a data breach had occurred. However, it appears that the data protection team was engaged via email by the Digital & Direct Risk Team on 24 May 2022, "*on foot of the Digital & Direct Risk Teams review of the call transcripts with the bad actor by the Digital & Direct Team*" and that a "*risk event was also logged by the Digital & Direct Risk Team on 24 May 2022 (at 16:38) on the GRC system in order to flag a potential personal data breac*h." In this respect, the notification to the Data Protection Team was preceded by a detailed fraud investigation, which included listening to all relevant call transcripts and which concluded on 24 May 2022 (at 13:46). On foot of this, "*PTSB had a reasonable degree of certainty that, in addition to a fraudulent attack on PTSB and the customer, a personal data breach had also occurred in relation to the customer's bank account*." The DPC is therefore satisfied that PTSB did not meet its obligations to determine whether a breach had occurred in a timely manner and notify the DPC of the data breach without undue delay and where feasible not later than 72 hours of having become aware of it.

141. For the above reasons, the DPC therefore finds that PTSB infringed Article 33(1) GDPR.

H. Findings

142. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, findings that PTSB:

- infringed the principle of integrity and confidentiality of Article 5(1)(f) GDPR by failing to ensure appropriate security of the personal data related to accounts of its customers using appropriate technical and organisational measures;

- infringed Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data within the Open24 Contact Centre; and
- infringed Article 33(1) GDPR by its failure to notify the DPC without undue delay and within 72 hours of becoming aware of the Breaches.

I. Decision on Corrective Powers

143. 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) GDPR and, if so, which corrective powers.

144. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. 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…"*

145. Having carefully considered the infringements identified in this 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 deemed appropriate to impose in order to address the infringements in the particular circumstances are:

- A reprimand to PTSB in respect of its infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR;
- One administrative fine in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR; and
- One administrative fine in respect of the infringement of Article 33(1) GDPR.

146. Set out below are further details in respect of each of the corrective powers that the DPC has decided to exercise and the reasons why it has decided to exercise them.

J. Decision on Reprimand

147. 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*".

148. The DPC hereby issues PTSB with a reprimand in respect of its infringements of Articles 5(1)(f), 32(1), and 33(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The reprimand will contribute to ensuring that PTSB and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations under the GDPR.

K. Decision on Order to Bring Processing into Compliance

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

"*…to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period*".

150. In circumstances where it has been found that the processing at issue was not in compliance with the GDPR, the DPC has the ability to make an order pursuant to Article 58(2)(d) GDPR. Due to the remedial actions taken by PTSB in response to the Breaches, the DPC does not consider it appropriate, necessary and proportionate to make an order for PTSB to bring its processing into compliance with Articles 5(1)(f), 32(1) and 33(1) GDPR. In this regard, the DPC acknowledges PTSB's ongoing remedial actions, as outlined in its submissions throughout the Inquiry. The DPC's acknowledgement of those improvements does not however relieve PTSB of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by its processing.

L. Decision on Administrative Fines

151. 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*".

152. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[81] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

153. As the DPC has identified infringements of the GDPR, the DPC will decide whether to impose an administrative fine 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'**),[82] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines (the '**A29WP Fining Guidelines**'),[83] which have been endorsed by the EDPB.

154. In its submissions of 26 September 2025, PTSB stated that the EDPB Fining Guidelines "*do not have legal status like Article 83(2) GDPR*" and that the DPC should have regard to this "*where wording within the EDPB Guidelines goes beyond the text and spirit of Article 83(2) GDPR.*"[84] In this regard, Article 70(1) GDPR provides that the EDPB shall ensure the consistent application of the GDPR. To that end, it shall, *inter alia*, "*issue guidelines, recommendations and best practices in order to encourage consistent application of [the GDPR]*" and "*draw up guidelines for supervisory authorities concerning […] the setting of administrative fines pursuant to Article 83*". The EDPB Fining Guidelines do not impose new standards or requirements but, rather, outline the manner in which individual supervisory authorities might achieve a harmonised approach to the assessment of fining matters. They reflect the detailed assessment that is required to be carried out pursuant to Article 83 GDPR. As noted in the guidelines, the calculation of the amount of the fine is at the discretion of the relevant supervisory authority, subject to the rules provided for in the GDPR, which requires that the amount of the fine in each individual case shall be effective, proportionate, and dissuasive.

155. The calculation of any administrative fine is based on a specific evaluation carried out in each case, within the parameters provided for by the GDPR.[85] While the DPC considers it

[81] GDPR, rec 148.
[82] Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 2.1, adopted on 24 May 2023.
[83] WP253.
[84] PTSB submissions on Draft Decision, 26 September 2025, p.3
[85] EDPB Fining Guidelines, page 3.

appropriate to have regard to the EDPB Fining Guidelines as an important interpretative tool in ensuring the consistent application of the GDPR, this Decision contains a comprehensive explanation of the manner in which the DPC has applied each of the Article 83 criteria to the individual circumstance of this particular case.

156. As a first step, the DPC will thus 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

157. 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 deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…*"

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

158. 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 the processing operations that PTSB carries out on personal data in the context of its Open24 Contact Centre.

159. 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. PTSB has been found to have infringed Articles 5(1)(f), 32(1) and 33(1) 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)(f), 32(1) and 33(1) 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.

160. 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

161. 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.

162. 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*."[86]

163. The nature of the processing is PTSB's processing of personal data – including financial data – through its Open24 Contact Centre. PTSB is a leading provider of personal and business banking services in the Irish market and the Open24 Contact Centre functions as PTSB's primary point of customer contact. It allows customers to take actions such as checking their account balance, transactions, or standing orders or make fund transfers and payments to other designated accounts.

164. 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*

[86] EDPB Fining Guidelines [53.b.i].

processing in terms of the allocation of resources by the data controller… The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor."[87]

165. The scope of the processing concerned is broad in nature. As PTSB's primary point of customer contact, a large volume of calls are received from customers seeking to take action in relation to their account, including the amendment of account details and making of payments. In this respect, PTSB has advised that the Open24 Contact Centre received [redacted] million calls during 2022 and that it recruited and trained over [redacted] staff specifically to work within the Open24 Contact Centre in the same period.[88] The quantity of personal data potentially stored on any given account was also broad in scope and sensitive in nature, including data subject identity, contact details, and economic and/or financial data. The likelihood of any error resulting in a data breach was therefore high. The DPC has had regard to the fact that, insofar as the DPC is aware, only three accounts were affected by the Breaches considered in this Decision, however a much wider range of data subjects were at risk in light of the broad scope of the processing.

166. 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 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).*"[89]

167. The purpose of the processing identified herein was to facilitate customers carrying out a range of banking functions via telephone. This included checking their account balance, information about transactions, information regarding standing orders, fund transfers and

[87] EDPB Fining Guidelines [53.b.ii].
[88] PTSB response to Statement of Issues 24 February 2024 p1-2.
[89] EDPB Fining Guidelines [53.b.iii].

payments to other designated accounts, bill payments and requesting account statements for current, savings and loan accounts. The purposes of the processing relate to the core functions of PTSB.

168. 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*."[90]

169. The number of data subjects affected by the Breaches identified herein is three. However, all PTSB customers using the Open24 Contact Centre were potentially affected by the infringements regarding the lack of appropriate security caused by vulnerabilities in PTSB's procedures and policies, training, and technical and organisational measures. The lack of appropriate technical and organisational measures means that these other PTSB customers were vulnerable to a loss of control of their personal data, its accuracy, or in extreme cases to theft, fraud or financial loss due to the actions of other malicious actors.

170. 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*

[90] EDPB Fining Guidelines [53.b.iv].

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."[91]

171. In this case, the level of damage suffered is high. In two instances, data subjects suffered considerable financial loss.[92] In all instances, the three data subjects concerned suffered loss of control over their personal data, were put at increased risk of additional theft, fraud, or financial loss due to the disclosure of their personal data by PTSB, were forced to close their accounts and were therefore not free to exercise control over their monies held with PTSB. In its submissions of 26 September 2025, PTSB submitted that "*it is not clear*" how the level of harm was considered high, and that it should not be held responsible for the fraudulent attacks committed on the data subjects prior to the Breaches. PTSB further reiterated that it had provided a full refund to the affected data subjects and noted that, rather than being forced to close their accounts with PTSB, the affected data subjects were informed that "*PTSB would no longer be in a position to continue to guarantee the safety of the account in the future*."[93]

172. In this regard, the DPC notes that, as detailed above, while bad actors came into possession of customer information prior to contacting PTSB, the information should not have been sufficient to access their accounts. Repeated data breaches ultimately occurred due to failures by PTSB staff/ agents in following identity verification protocols. The failings which the DPC has concluded above were enabled by a lack of appropriate technical and organisational measures. The DPC has not sought to hold PTSB responsible for any prior attacks committed on the data subjects, but rather for the failings in its own technical and organisational measures. Due to those failings, information on data subjects was repeatedly disclosed to bad actors, bank account details were changed and, in two cases, numerous fraudulent transactions occurred. As a result of the Breaches, data subjects were also without access to their bank accounts for a period of time.

---

[91] EDPB Fining Guidelines [53.b.v].
[92] The affected customers were later refunded the monies taken from their bank accounts. In BN-22-5-469, the fraudulent transactions, totalling €34,087.82 occurred between 20 and 23 April 2022. The refund was made available on 27 June 2022 and collected by the customer in branch on 5 July 2022. In BN-22-5-497, the fraudulent transactions, totalling €10,000, occurred on 7 May 2022 and a refund was provided by PTSB on 9 June 2022.
[93] PTSB submissions on Draft Decision, 26 September 2025, pages 9-11.

173. The DPC acknowledges that the affected customers were later refunded (and has considered this under Article 83(2)(c) below, in addition to other measures taken by PTSB to secure the relevant accounts), however, this took a significant period of time to occur (in excess of one month in both cases) and data subjects were without access to those funds in the interim. While the DPC also acknowledges that the prior fraudulent attacks contributed to PTSB advising the data subjects that it could not guarantee the safety of their accounts, the Breaches, for which PTSB was ultimately responsible, undoubtedly played a key role in the compromising of those accounts and directly led to this additional damage suffered by the data subjects. In the circumstances, the DPC is satisfied that it has appropriately considered the level of damage to data subjects.

174. In its submissions of 26 September 2025, PTSB further stated:

> "*[T]he DPC considers in detail the nature, scope and purpose of the processing of customer personal data within Open 24 generally. The DPC place significant reliance on the EDPB Fining Guidelines in this context. However, it is respectfully submitted that the DPC provides comparatively limited analysis concerning the legal principles, within articles 5(1)(f), 32(1) and 33(1) of the GDPR, to the specific factual circumstances surrounding the nature and gravity of the actual alleged infringement set out in the Notice of Commencement of an Inquiry dated 24 August 2022 (i.e. three specific incidents the subject of the Inquiry) including the prior customer-initiated data compromise involving the same three customers the subject of the Inquiry*."[94]

175. However, as detailed above, the 'processing concerned' in this Article 83(2) analysis should be understood as meaning the processing operations that PTSB carries out on personal data in the context of its Open24 Contact Centre. Furthermore, 'the infringements' 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)(f), 32(1) and 33(1) GDPR. In this regard, the Inquiry considered, *inter alia*, the question of whether PTSB infringed Articles 5(1)(f) and 32(1) GDPR in respect of its processing of personal data in the Open24 Contact Centre and detailed analysis on this issue is set out above. The Notice of Commencement clearly details that:

[94] PTSB submissions on Draft Decision, 26 September 2025, p.4

> "*[T]he scope of the inquiry will focus on PTSB's organisational and technical measures that are in place to ensure security and accuracy of the personal data involved, particularly in relation to its telephone call handling processes. The Inquiry will also examine associated policies and procedures that are in place that identify any risk to data subjects and the organisational and technical measures to address those risks*."

176. PTSB was similarly advised of the material scope by way of the Statement of Issues and Draft Decision. While the Breaches are a highly relevant consideration in this regard (and are central with regard to the infringement of Article 33(1) GDPR for failing to notify the DPC in the required timeframe), it is appropriate that the DPC has regard to the full extent of the processing as considered in the Inquiry, which encompasses the processing of customer data in the Open24 Contact Centre and the absence of appropriate technical and organisational measures in this regard.

177. The DPC has concluded in this Decision that PTSB infringed *inter alia*, Article 5(1)(f) GDPR and Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data within the Open24 Contact Centre. In submitting that the DPC provides insufficient analysis concerning the "*the nature and gravity of the actual alleged infringement*" and has placed "*significant reliance on the EDPB Fining Guidelines in this context*", the submission of PTSB misstates the nature of both the 'processing concerned' and the 'infringement' as detailed throughout this Decision, which is not limited in the manner suggested by PTSB (i.e. in all circumstances to three specific incidents rather than a broader consideration of the technical and organisation measures in the Open24 Contact Centre). Furthermore, as is required by Article 83(2)(a) GDPR, the DPC has assessed the full extent of the nature, scope, and purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, in this section, before proceeding to consider below the nature, gravity and duration of the infringements in light of this.

The nature of the infringements

178. 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".[95]

179. In line with 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.[96]

180. The nature of the infringement identified herein regarding Articles 5(1)(f) and 32(1) GDPR comprises a failure of PTSB to comply with its obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of its processing operations via its Open24 Contact Centre. The objective of Articles 5(1)(f) and 32(1) GDPR is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of natural persons because of the potential for damage to them where personal data breaches occur, leading to, *inter alia*, unavailability or destruction of essential personal data or unauthorised access, alteration or disclosure of that personal data. Therefore, compliance with Articles 5(1)(f) and 32(1) is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious consequences in that it has the potential to result in damage to natural persons.

181. The nature of the infringement identified herein regarding Article 33(1) comprises a failure on the part of PTSB to notify the DPC of personal data breaches within the appropriate time after the controller ought to have become aware of them. The nature of this infringement must be assessed in light of the purpose of Article 33(1), which is to ensure prompt notification of personal data breaches to supervisory authorities. This enables a supervisory authority to assess the circumstances of the data breach, including the risks to natural persons. It can then decide whether the interests of those persons must be safeguarded to the extent possible, by mitigating the risks to them arising from a data breach,[97] for example by ordering a controller to communicate a personal data breach to affected data subjects under Article 34(4) or 58(2)(e) of the GDPR.

[95] EDPB Fining Guidelines, [53.a].
[96] Article 83(2)(a).
[97] Recital 85 GDPR.

182. In its submissions of 26 September 2025, PTSB submitted that "*the nature of the alleged infringements - should be considered within the particular factual context in which these incidents arose within Open 24 and, as the DPC acknowledges in the Draft Decision, the 'low number of data subjects' involved in these three data breaches the focus of the Inquiry*."[98] In this regard, the DPC has had detailed regard to the nature, scope and purposes of the processing concerned (i.e., the processing operations that PTSB carries out on personal data in the context of its Open24 Contact Centre), when considering the nature of the infringements and, in addition, considered above the number of data subjects affected by the infringements and the level of damage suffered by them. This is required by Article 83(2)(a) GDPR.

183. PTSB further asserted that, in considering the nature of the infringement, the DPC has not had sufficient regard to "*the factual context surrounding the three specific PTSB data breaches including the prior inadvertent disclosure of personal data by these three affected customers.*"[99] The DPC considers the fact that the relevant personal data breaches were contributed to by "*prior customer-initiated data compromise*" to be of more limited relevance in the specific circumstances of the infringements. Whilst bad actors were successful in obtaining certain information concerning the data subjects affected by the Breaches, prior to those bad actors contacting PTSB, the information obtained should not have been sufficient to compromise those data subjects' PTSB accounts and/or led to the disclosure of additional information concerning them by PTSB. PTSB as a controller was under an obligation to implement appropriate technical and organisational measures in order to ensure the appropriate level of security and to report data breaches as they arose without undue delay. As detailed above, the DPC has found that PTSB failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data within the Open24 Contact Centre and failed to meet its obligations to notify the DPC of the Breaches within the timeframe required by law.

[98] PTSB submissions on Draft Decision, 26 September 2025, p.4
[99] PTSB submissions on Draft Decision, 26 September 2025, p.6.

The Gravity of the Infringements

184. 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.[100]

185. The gravity of the infringement of Articles 5(1)(f) and 32(1) of the GDPR is moderate in circumstances where the infringements resulted in the Breaches and, in light of the nature, broad scope and purposes of the processing, put a large number of data subjects at risk. The infringement directly impacted the confidentially, integrity and availability of the data of the data subjects concerned and led to a significant financial loss to two of those data subjects. However, the DPC also acknowledges that PTSB accurately assessed the high risk of the processing and put in place a range of policies to mitigate the risk. Similarly, PTSB closed the affected accounts and reimbursed the data subjects for the financial loss they suffered in BN 22-5-469 and BN-22-5-497. Nonetheless, in light of the failure to implement a number of those policies in practice, and the flaws identified in this Decision, the DPC considers that the gravity of PTSB's failure to implement sufficient and appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of customer data to be moderate.

186. The infringement of Article 33(1) GDPR concerned the personal data of a low number of data subjects and the DPC has found that there was an infringement of the GDPR in PTSB's failure to notify the DPC of the Breaches at the required time. Any assessment of the gravity of the infringement must necessarily take account of how it interfered with the overall purpose of notifying a personal data breach to the supervisory authority. In this case, there was a delay in notifying each of the Breaches to the DPC which, in turn, delayed the assessment by the DPC of the Breaches and their potential impact, thereby interfering with this legislatively mandated additional layer of protection. The DPC accepts, however, that despite the potential for damage to data subjects arising from the potential for consequent delays in actions taken by the DPC to safeguard/ mitigate risks to data subjects, as matters materialised, there was no additional direct damage to data subjects arising from the delayed notification. Furthermore, the infringement must be assessed in light of the fact that it is also usually capped at the lower threshold under Article 83(4) GDPR. Nonetheless, as outlined above, the DPC considers that PTSB did not meet its obligations to determine

[100] Article 83(2)(a).

whether personal data breaches had occurred in a timely manner and this led to an increased risk for data subjects that were subject to the Breaches, including of additional fraud which would likely have been addressed had notification to the DPC within 72 hours occurred. The Breaches further illustrated significant non-adherence to PTSB's own Data Security Breach Procedure. In those circumstances, and in light of the importance of the notification process in protecting the rights and freedoms of data subjects, the gravity of the finding of an infringement of Article 33(1) is moderate.

187. In its submissions of 26 September 2025, PTSB took issue with the DPC's conclusion that the infringements put a large number of data subjects at risk, in light of the broad scope of the processing concerned. PTSB stated that that when considering the gravity of the infringements by PTSB pursuant to Article 83(2)(a) of the GDPR, "*the DPC is required to have 'due regard' to 'the number of data subjects affected, and the level of damage suffered by them [i.e. the affected data subjects[sic]*.'"[101] It asserts, in this regard that, "*the provision is objectively clear in that there were only three specific data subjects affected in the context of the scope of the Inquiry*." Elsewhere in its submissions on this point, PTSB refers to "*the three specific data subjects the subject of the inquiry"* and the "*three specific incidents under inquiry*". This illustrates a misunderstanding on the part of PTSB of the nature of its obligations under Articles 5(1)(f) and 32 GDPR.

188. In order for PTSB to comply with Articles 5(1)(f) or 32 GDPR, it was not under an obligation to eliminate all risk of a personal data breach occurring, insofar as a strict liability standard is not imposed by the GDPR. Put otherwise, the infringements of Articles 5(1)(f) and 32 GDPR in this instance do not solely stem from the existence of the Breaches, but rather the failure to implement appropriate technical and organisational measures for ensuring the appropriate level of security in the Open24 Contact Centre. This is examined in detail by way of issue 1 above, which is manifestly not limited to a consideration of security measures in place insofar as they relate to three specific data subjects only, but rather concerns the Open24 Contact Centre in general. Therefore, while the number of data subjects affected by the failure to notify the Breaches within the legally required timeframe was three in number, all PTSB customers using the Open24 Contact Centre were potentially affected by the infringements regarding the lack of appropriate technical and organisational measures in the Open24 Contact Centre.

[101] PTSB submissions on Draft Decision, 26 September 2025, p.6

189. Furthermore, the DPC notes that the EDPB Fining Guidelines support this position and state that when considering the number of data subjects affected, in assessing the gravity of an infringement, supervisory authorities should consider:

> "[t]*he number of data subjects concretely but also potentially affected. The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor*."[102]

190. With regard to the infringement of Article 33(1), the DPC has detailed above that this concerned the personal data of a low number of data subjects and factored this into its assessment of the gravity of the infringement. However, the DPC does not accept the submission of PTSB that the low number of data subjects affected necessarily means that the overall gravity of the infringement must be assessed as low. This is one of several factors relevant to the assessment of gravity and the DPC has taken it into consideration in its examination above.

The duration of the infringements

191. 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*."[103]

192. 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.[104]

[102] EDPB Fining Guidelines, [53.b.iv].
[103] EDPB Fining Guidelines [53.c].
[104] A29WP Fining Guidelines, p11.

193. 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.[105]

194. In this case, the duration of PTSB's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing concerned commenced at the application of the GDPR on 25 May 2018 when the GDPR became law. The obligation to implement and be able to demonstrate the appropriate organisational and technical measures applied from 25 May 2018. The infringements of Articles 5(1)(f) and 32(1) GDPR found here were ongoing for the entirety of the temporal scope in circumstances where PTSB failed to implement appropriate measures required by those provisions for the entirety of that time frame. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement of Articles 5(1)(f), and 32(1) GDPR lasted at least from 25 May 2018 until 27 May 2022.

195. Regarding the duration of the infringement of Article 33(1) GDPR, as outlined above, the DPC finds that there are no circumstances concerning the Breaches that justify a failure to notify the DPC without undue delay and within 72 hours of when PTSB became aware of them. This is especially the case in circumstances where the DPC has also found that PTSB did not proceed with all due diligence to ensure that the Breaches were identified in a timely manner and ought to have been aware of them from an earlier point in time. As detailed in paragraph 140, the Breaches were notified to the DPC on 26 May 2022 (BN-22-5-459) and 27 May 2022 (BN-22-5-469, and BN-22-5-497), while the respective fraud incidents were first brought to the attention of PTSB on 8 April 2022 (BN-22-5-459), 3 May 2022 (BN-22-5-469) and 9 May 2022 (BN-22-5-497).

196. While PTSB ought to have taken prompt action to ensure that it was aware of the Breaches in a timely manner, this did not occur. It appears that the existence of the personal data breaches in BN-22-5-469 and BN-22-5-497 was fully established during a subsequent fraud investigation, and at the very latest by 23 May 2022 and 24 May 2022, whereas they ought to have become apparent to PTSB shortly following contact from the affected data subjects. In the case of BN-22-5-459, PTSB was aware of the circumstances of the breach by 16 April 2022 following a call from the data subject and subsequent investigation. While the DPC considers that the delay in PTSB determining with a reasonable degree of certainty that

[105] Article 83(2)(a).

breaches had occurred was significant, and the notifications each occurred outside the relevant statutory timeframe once this occurred, it is acknowledged that the delay in notification once PTSB was subjectively aware of the Breaches is less significant in the cases of BN-22-5-469 and BN-22-5-497. In BN-22-5-459, the DPC considers the breakdown in communications and resultant delay in notification to be more significant. Indeed, had the affected data subject not made a complaint and further followed up, it appears that the breach may not have been discovered or brought to the attention of the Data Protection Team or ultimately reported to the DPC. The DPC finds the duration of the infringement is at a relatively lower level of the scale of culpability in the circumstances in BN-22-5-469 and BN-22-5-497. However, given the short overall timeframe generally permitted for breach notifications i.e. 72 hours or three days, it is not insignificant. In BN-22-5-459, the delay is more significant and of moderate duration.

197. In its submissions of 26 September 2025, PTSB asserted that the duration of the infringements of Articles 5(1)(f) and 32(1) GDPR "*should be limited to the period of the three incidents from 8 April (earliest awareness of a possible personal data breach)to 29 June 2022 (final remediation steps carried out including team briefing delivered by the Data Protection Team).*"[106] However, the occurrence of the Breaches does not limit the duration of the infringements in the manner suggested by PTSB. The obligation to implement and be able to demonstrate the appropriate organisational and technical measures applied from 25 May 2018 and the infringements of Articles 5(1)(f) and 32(1) GDPR were ongoing for the entirety of the temporal scope. The DPC is therefore satisfied that the duration of those infringements has been appropriately considered.

198. In relation to the duration of the infringement of Article 33(1) GDPR, PTSB contend that there is "*a rational justification for this delay*" (in notification) as:

> "*…the focus of PTSB's Fraud Team was investigating and determining the scale of the fraud attack committed on the affected customers. The Fraud Team were actively taking steps to halt any further fraud and support the three affected customers. To determine whether this was also a data breach the Digital & Direct Risk Team was required to listen to a significant number of calls from the bad actors*."[107]

[106] PTSB submissions on Draft Decision, 26 September 2025, p.11.
[107] PTSB submissions on Draft Decision, 26 September 2025, p.12

199. PTSB further stated that its delay in submitting the breach notifications did not materially impact its ability to respond to the incidents and did not detrimentally impact the affected data subjects. PTSB refers to mitigating measures that it put in place following the Breaches (which the DPC has acknowledged and accounted for elsewhere in this Decision) and submits that the delay in notification:

> "[S]*hould be viewed in light of the factual context including (i) once each of the three frauds were identified by PTSB, the Fraud team took swift steps to secure those customer accounts by putting transaction holds on them (ii) the money lost by two of the three data subjects involved was quickly refunded by PTSB, and (iii) as transactions holds were placed on the affected accounts well in advance of the breach notification made to the DPC, the level of risk to the three affected customers was not increased by the delayed reporting to the DPC*."[108]

200. Article 33(1) GDPR provides that a personal data breach should be reported by the controller without undue delay and, where feasible, not later than 72 hours after becoming aware of a breach. There is no provision for a derogation from the timeline provided for in Article 33(1) GDPR for the specific circumstances outlined by PTSB, whereby a controller may independently consider that it has subsequently remedied the issues which may have allowed further harm to occur and delay notification on that basis. The obligation to report breaches promptly is an important measure to ensure accountability of controllers and, as Recital 87 GDPR makes clear, an important purpose of Article 33(1) is to enable the supervisory authority to intervene in accordance with its tasks and powers. A failure to notify without undue delay can deprive data subjects of this legislatively mandated additional layer of protection, whereby a supervisory authority can consider using its powers to protect the rights and freedoms of data subjects. The DPC is satisfied that PTSB did not take the necessary action to ensure that it was aware of the Breaches in a timely manner. PTSB was not entitled to suspend its consideration of whether data breaches may have occurred, and delay notifying the supervisory authority, pending completion of a separate and lengthy fraud investigation. Indeed, the DPC notes that, in the circumstances of each of the Breaches, PTSB failed to comply with its own internal Data Security Breach Procedure in so doing. The DPC is also satisfied that once PTSB's Data Protection Team were made aware of the incidents, after a detailed fraud investigation had concluded, there were

[108] Ibid.

no circumstances which justified a further delay in notification in excess of 72 hours. The DPC is satisfied that it has appropriately considered the duration of the infringements of Article 33(1) in full knowledge of the facts surrounding each of the Breaches, which are outlined in detail above.

201. Whilst the DPC also acknowledges that the money lost by two data subjects was later refunded by PTSB, the DPC does not consider this to be of particular relevance to the duration of the infringements. However, the DPC has noted the mitigating effect of this measure under its consideration of Article 83(2)(c) below.

Assessment of Article 83(2)(a) GDPR

202. Taking account of all of the factors assessed in this section, the DPC assesses the infringement of Articles 5(1)(f) and 32(1) GDPR to be of a moderate gravity and of a substantial duration. PTSB's processing of personal data via its Open24 Contact Centre in the absence of sufficient oversight, training and the implementation of appropriate organisational and technical measures resulted in unauthorised access, alteration and unauthorised disclosure of personal data to third parties and subsequent fraud. It also directly led to loss of control over personal data and financial loss and put a larger cohort of data subjects at risk.

203. With regard to the infringement of Article 33(1) GDPR, the Breaches resulted in a high risk to the rights and freedoms of natural persons, as evidenced by the financial fraud perpetrated and so should have been notified to the DPC within 72 hours of PTSB becoming aware of them. Such notifications are crucial for enabling supervisory authorities to assess the circumstances of a data breach, including the risks to data subjects, and decide whether action is required to mitigate those risks. PTSB did not proceed to determine that the Breaches had occurred in a timely manner, and once it belatedly did so, there was an additional delay in notification. Taking account of all of the factors assessed in this section, the DPC assesses the infringement to have a moderate gravity. As stated above at paragraph 196, the DPC finds that the duration of the infringement is at a relatively lower level of the scale of culpability in respect of BN-22-5-469 and BN-22-5-497. In respect of BN-22-5-459, the delay is more significant and thus represents an infringement of moderate duration.

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

204. The A29WP Fining Guidelines state:

> "[I]*n 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*."[109]

205. 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'.*[110] *In case of an intentional infringement, 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*."

206. PTSB's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing concerns its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concern the lack of the implementation of appropriate technical and organisational measures for the duration of the infringement. In order to classify this infringement as intentional, the DPC must be satisfied that (i) PTSB wilfully omitted to implement appropriate technical and organisational measures and (ii) that it knew at the time that the measures that it implemented were not sufficient to meet the standards required by Articles 5(1)(f) and 32(1) GDPR.

207. While PTSB's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 32(1) GDPR, the DPC does not consider that PTSB knew that the measures implemented were not sufficient at the time such as to render the infringement intentional. Notwithstanding the absence of an intentional infringement, in the circumstances, PTSB ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 32(1) GDPR. For example, PTSB ought to have been aware that its removal of the extra training procedures regarding calls received from [redacted] may

[109] A29WP Fining Guidelines, p11.
[110] Footnote from EDPB Fining Guidelines: *Guidelines WP 253 p 12.*

lead to the risk of staff error in handling such calls and that the technical and organisational measures employed in the Open24 Contact Centre were not sufficiently robust to respond to the high risk and therefore presented a weak point open to exploitation by bad actors. Similarly, PTSB should have been aware that some of the audit and training measures in place for PTSB staff and agents may not have been robust enough to correspond to the high level of the risk of unauthorised access by malicious actors. The DPC therefore finds that the infringement was of a negligent character and, in light of the level of negligence present, the DPC finds this factor to be aggravating to a moderate degree in considering the need for an administrative fine and the amount of any such fine.

208. In relation to the infringement of Article 33(1) GDPR, PTSB ought to have been aware of the obligation to examine the data protection aspects of the incidents in a prompt manner and the repeated failure to do so was indicative of a systemic issue. The lack of escalation by teams dealing with the fraud aspects of the Breaches at an appropriate point, and as outlined in PTSB's own procedures, contributed and resulted in the failure to deal with the personal data breaches correctly at the time at which they occurred and led to a significant delay in notification. PTSB also ought to have been aware of its obligation to inform the DPC within 72 hours of becoming aware of a data breach. The DPC therefore finds that the infringement was of a negligent character and, in light of the level of negligence present, the DPC finds this factor to be aggravating to a moderate degree.

209. In line with the approach in the EDPB Fining Guidelines, the DPC has considered this factor below, in addition to those in Articles 83(2)(a) and (g) GDPR, in determining the overall level of seriousness of the infringements, when considering the amount of the administrative fine to be imposed. To be clear, the DPC has not additionally considered this factor as further aggravating beyond this but rather thereafter considered the remaining aggravating and mitigating factors in Article 83(2) GDPR before determining the level of administrative fines to be imposed.

210. In its submissions of 26 September 2025, PTSB stated that, with regard to the infringements of Article 5(1)(f) and 32(1) GDPR:

> "*While it is accepted that a finding of intentional behaviour may constitute an aggravating factor, where the DPC's finding is that of negligence (as is the position here), then it is respectfully submitted that, for the DPC to conclude that this negligence finding represents an aggravating factor at all (leaving aside that this could amount to a finding of "aggravating to a moderate degree") this does not*

appear to be consistent with the purpose and spirit of article 83(2)(b) of the GDPR when the surrounding circumstances are considered."[111]

211. PTSB further asserts that the DPC did not elaborate on what was meant by the level or degree of negligence, that Article 83(2)(b) only provides for the DPC to conclude whether the alleged infringement was negligent or intentional (and not an aggravating factor) and that in a previous decision of the DPC concerning Bank of Ireland the DPC did not consider this as an aggravating factor despite concluding that negligence was present. On this point, PTSB also submits that the DPC should account for the fact that the types of attacks as considered in this inquiry are "*unavoidable*", involved bad actors who were armed with a significant amount of customer data and involved isolated human error by PTSB staff/ agents. For completeness, the DPC notes that PTSB also submits that it is also relevant that it took prompt action in identifying the root causes of the Breaches and adopting measures to prevent a reoccurrence. However, this is dealt with separately under the DPC's consideration of Article 83(2)(c), in considering the action taken to mitigate the damage suffered by data subjects following the Breaches.

212. In respect of the infringements of Article 33(1) GDPR, PTSB stated that it appeared that the DPC did not have sufficient regard to the factual circumstances relating to the reason for the delayed notification to the DPC or when viewed in the context of a "*sophisticated and significant fraudulent attack committed by bad actors on PTSB and its customers at this time*".[112] In this regard, PTSB notes that its fraud team were required to engage with its Digital and Direct Risk team, which thereafter were required to conduct a review of the relevant accounts and listen to all relevant call recordings. PTSB further notes that the delay in the notification in BN-22-5-497 was minimal in nature.

213. Based on the above considerations, PTSB therefore submits that the level of negligence should be regarded as neutral.

214. In this regard, Article 83(2) GDPR is clear that when deciding to impose an administrative fine, *and the amount of any such fine,* the DPC shall have due regard to, *inter alia*, the intentional or negligent character of the infringement. As noted above, the EDPB Fining Guidelines further note that supervisory authorities may attach weight to the degree of negligence and, at best, negligence could be regarded as neutral.[113] The DPC considers that

[111] PTSB submissions on Draft Decision, 26 September 2025, p.13
[112] PTSB submissions on Draft Decision, 26 September 2025, p.14
[113] EDPB Fining Guidelines [56].

its analysis at paragraphs 207 and 208 illustrates, with reference to specific examples, that PTSB's technical and organisational security measures at the time of the Breaches did not meet the standard required under Article 5(1)(f) and 32(1) GDPR, and that PTSB was or ought to have been aware of same. While the failure of PTSB to meet its obligations was not intentional, the DPC considers that PTSB ought to have been aware that the measures implemented were not sufficient to meet its obligations under the GDPR and considers that PTSB was negligent in failing to modify existing measures or to implement further appropriate measures.

215. In particular, and as outlined in detail in the assessment of Issue 1 above, the DPC is satisfied that PTSB appropriately assessed the high risks inherent in the processing carried out in the Open24 Contact Centre - indeed, in its submissions, PTSB has described the type of attacks considered in the Inquiry as "*unavoidable*" and a "*continuing external threat*". Given the proliferation of information about individuals online and the availability of information to bad actors through, for example, prior data breaches, attacks such as those considered in this Decision form an obvious part of PTSB's external threat environment. However, having correctly assessed the high risks, the technical and organisational measures subsequently implemented by PTSB in the Open24 Contact Centre fell short in a range of significant respects and were not sufficiently robust to respond to entirely predictable attacks which were highly likely to arise in the circumstances.[114] Those shortcomings were exploited during the Breaches and led to increased risks for a much larger cohort of data subjects whose personal data was processed. While the DPC accepts that the bad actors came into possession of customer data prior to contacting PTSB, such information generally should not on its own have been sufficient for them to obtain or change account details and thereafter fraudulently make use of funds in those accounts. It was ultimately PTSB's failure to implement appropriate technical and organisational measures that led to the Breaches. The DPC is therefore satisfied that it has detailed the reasons why this factor cannot be regarded as neutral and weighs in the balance in considering both the need for an administrative fine, and the amount of any administrative fine, based on the particular facts of this case.

216. With regard to references to other cases concerning Articles 5(1)(f) and 32(1) GDPR, the DPC notes, firstly, that Articles 58(2)(i) and 83(2) GDPR each expressly state that administrative fines depend on the circumstances of the individual case. In coming to the

[114] See, for example, paragraphs 86-88, 92-94, 101-102, 109-110 and 112-114 above.

conclusions above, the DPC has considered the particular facts of this case. It is well established that negligence can either be an aggravating factor or a neutral factor, depending on the circumstances of the case. This is inherently a case-specific analysis. For the reasons set out in this Decision, the DPC finds that the degree of negligence on the part of PTSB is an aggravating factor in the particular circumstances.

217. In respect of the infringements of Article 33(1) GDPR, the DPC has considered the circumstances of each of the specific breaches in detail in determining that PTSB did not meet its obligations to determine whether data breaches had occurred in a timely manner and did not notify the DPC of each of the data breaches without undue delay, and within 72 hours of when its Data Protection Team belatedly became fully aware of them. The DPC notes that PTSB did not adhere to its own Data Security Breach Procedure in delaying its consideration of the potential data breach aspects of the incidents and, in one of the incidents (BN-22-5-459), its Data Protection Team only appear to have become aware of the incident, and later notified the DPC of same, as the data subject followed up with a complaint. This illustrates a level of negligence that must be strongly discouraged.

218. While, in BN-22-5-469 and BN-22-5-497, the delay in notification once PTSB was fully aware of the Breaches is less significant (and has been considered above by the DPC), PTSB did not proceed with due diligence in determining that the Breaches had occurred and in notifying the DPC in a timely manner. For example, while PTSB refers to the circumstances of BN-22-5-497 as indicative of a low level of negligence, it should be recalled that in this case, the relevant customer confirmed to PTSB that fraudulent transactions had occurred on 9 May 2022 and an examination of the relevant account revealed that the associated phone number had been changed, following calls made by a malicious actor between 6 and 7 May, with a fraudulent number associated with the account from 6 May to 10 May 2022. Transaction holds were placed on the customer's accounts on 9 May 2022 and the customer's phone number was reverted on the bank's systems. However, despite the obligation to notify data breaches without undue delay and within 72 hours, PTSB's Data Protection Team was not informed of a potential data breach until 24 May 2022 and notification to the DPC did not occur until 27 May 2022.

219. The DPC considers that the nature of each of the incidents, and subsequent contact with the affected customers, should clearly have put PTSB on notice that data breaches had potentially occurred and led to a prompt investigation. Furthermore, in each of the incidents, despite a delay in determining that data breaches had occurred, there was a subsequent delay in notification to the DPC once this became clear beyond question. The DPC is therefore satisfied that, contrary to the submission of PTSB, it has fully considered

the relevant factual background in determining that the infringements were of a negligent character and that this ought to be afforded moderate weight in determining the level of the fine to be imposed.

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

220. 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."*

221. PTSB put in place various mitigation measures after it discovered the Breaches. These measures included securing the affected customer accounts, providing a full refund of the financial loss incurred by the affected accounts, and offering advice to the data subjects on best practice in protecting their identity now and in the future in light of the potential for future targeted frauds.[115] PTSB additionally performed a specialised "lookback" exercise on the assurance evaluations completed with respect to the agents involved in the incidents the subject of the Inquiry. However, it is not always possible to correct a past lack of control retrospectively, as personal data has already been breached and data subjects suffered consequential damage as a result. Nonetheless, the actions taken by PTSB did make good the financial loss suffered as a result of the Breaches and sought to prevent further loss arising.

222. PTSB additionally made a number of substantial technical and organisational changes as a result of the Breaches and did so in a timely manner following their occurrence. These included a detailed review of the training process for new staff/agents, the relevant training manuals and security journeys, on foot of which a range of improvements were made. Those improvements included enhanced training for new staff/agents, the removal of the third security journey, extensive and immediate training for all staff/agents involved in the incidents around the security process, the introduction of technical enhancements to [redacted]

[115] PTSB response to Statement of Issues 24 February 2024 p10.

[redacted] and the reintegration into on-boarding training of a 2020 additional steps guide to be used prior to inputting a [redacted] mobile telephone number on the PTSB customer database.[116] Furthermore, a review of the process and procedures between the fraud team and the digital and direct risk team led to the introduction of a [redacted] Those measures were put in place swiftly after the investigation of the root cause of the Breaches and minimised the risks of any further breaches of a similar nature to the Breaches at issue, or any similar delay in notification, which the DPC considers to be of mitigating value. In its submission on the Issues Paper, PTSB further advised of a range of additional improvements that it has subsequently put in place. Having regard to the range of actions taken by PTSB in identifying the root cause of the Breaches, and seeking to very quickly put in place measures to prevent a reoccurrence, the DPC considers those actions to have a mitigating effect.

223. Overall, in light of the totality of the mitigating actions for the purpose of Article 83(2)(c) GDPR, the DPC takes the view that the actions were of mitigating value and must be ascribed moderate weight in the determination of the administrative fine.

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;

224. The key question in relation to this provision is whether PTSB ''*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 them by the Regulation.[117]

225. In its submissions, PTSB outlined the measures that it had in place to prevent any potential breach of data protection. The DPC has had full regard to those measures in this Decision. This Decision assesses whether PTSB complied with its obligations under Articles 5(1)(f) and 32(1) GDPR by implementing appropriate technical and organisational measures to ensure appropriate security of the personal data processed in the context of the Open24 Contact Centre. As stated above, the DPC finds that PTSB infringed those two provisions. Furthermore, the absence of the implementation of appropriate organisational measures contributed to the delay in notification to the DPC as the Data Protection Team were not

[116] PTSB response to Statement of Issues 24 February 2024 p21.
[117] EDPB Fining Guidelines, [77].

promptly notified of the potential personal data breaches. Even following their notification, the Data Protection Team delayed notifying the DPC. PTSB is obliged to ensure that it has appropriate measures in place to meet its obligations under Article 33(1) GDPR.

226. Against this backdrop, the DPC considers that PTSB holds a high degree of responsibility for this infringement and that the absence of the implementation of sufficiently robust technical and organisational measures must be deterred. It is clear that PTSB did not do 'what it could be expected to do' in the circumstances assessed in this Decision.

227. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against PTSB, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

228. In its submissions of 26 September 2025, PTSB submitted that, "*while human error by PTSB contributed towards the bad actors being able to commit a fraudulent attack on PTSB and these three customers*", it is relevant within this criterion to note that "*the bad actors were already in possession of and unlawfully processing a significant amount of personal information relating to the three affected customers* which was obtained through prior successful attacks."[118] As a result of this, PTSB submits that the degree of responsibility of PTSB should be considered as a mitigating factor.

229. While the DPC accepts that bad actors came into possession of some customer data prior to contacting PTSB, in the Inquiry, the DPC has examined the technical and organisational measures in the Open24 Contact Centre and found that they were not appropriate to respond to the high level of risk. It was the responsibility of PTSB as a data controller to ensure that appropriate measures were put in place, and the responsibility of PTSB to do so cannot be lowered due to the occurrence of prior attacks or human error. Had those measures been appropriate to respond to the level of risk present, no infringement of the GDPR would have occurred regardless of any prior attacks or human error - as noted above, a strict liability standard is not imposed by the GDPR and the occurrence of data breaches does not in itself mean that an infringement of Article 5(1)(f) or 32(1) GDPR has occurred. Similarly, it was solely the responsibility of PTSB to ensure that it implemented appropriate measures to meet its obligations under Article 33(1) GDPR and its responsibility to do so is

[118] PTSB submissions on Draft Decision, 26 September 2025, p.15

not lowered where prior attacks on data subjects may have occurred or in circumstances where human error may play a role in an underlying data breach. The DPC also observes that the nature of the prior attacks (postal interception and smishing) and human error (failure to adhere to basic security procedures in the absence of appropriate technical measures and training) were entirely predictable in this case and form part of the threat environment in which PTSB operates. The fact that those risks materialised, and exposed flaws in PTSB's technical and organisational measures, cannot lower its degree of responsibility.

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

230. In line with the EDPB Fining Guidelines, prior infringements are those already established before the decision (in the sense of Article 60 GDPR) is issued.[119] According to the A29WP Fining Guidelines, *'[t]his criterion is meant to assess the track record of the entity committing the infringement*.'[120]

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

232. In its submissions of 26 September 2025, PTSB submitted that, where a previous infringement is likely to constitute an aggravating factor, it follows that the absence of previous infringement by PTSB should constitute a mitigating factor in this context.[121]

233. The DPC does not accept this submission. The Article 83(2) GDPR criteria are not binary in nature such that, when assessed in the context of an infringement, they must be found to be either a mitigating or aggravating factor. While previous infringements can be considered aggravating, this must be determined on a case-by-case basis in view of the frequency and nature of any previous infringement(s), having regard to criteria such as the subject matter, time-frame and procedure in which the infringement was established.[122] The EDPB Fining Guidelines further state that the absence of any previous infringements

[119] EDPB Fining Guidelines, [82].
[120] A20WP Fining Guidelines p14.
[121] PTSB submissions on Draft Decision, 26 September 2025, p.15
[122] EDPB Fining Guidelines, [82]-[94].

"*cannot be considered a mitigating factor, as compliance with the GDPR is the norm"* and that *"if there are no previous infringements, this factor can be regarded as neutral."*[123]

234. Accordingly, the DPC considers this factor to be neutral in this case.

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;

235. The extent to which PTSB has cooperated with the inquiry is relevant to consider under this heading.[124] PTSB submitted breach notification forms in respect of the Breaches to the DPC and gave updates regarding PTSB's progress in remediating the Breaches. The DPC acknowledges PTSB's cooperation with the DPC during the course of the Inquiry. However, the DPC notes that PTSB was, in any event, under a duty, in light of Article 31 GDPR, to cooperate on request with the supervisory authority in the performance of its tasks. In this regard, the EDPB Fining Guidelines state that "*the ordinary duty of cooperation is mandatory and should therefore be considered neutral (and not a mitigating factor).*"[125]

236. The DPC notes that PTSB has made a number of substantial technical and organisational improvements to security as a result of the Breaches, to mitigate the adverse effects and prevent a recurrence, and has engaged with the DPC in this regard during the Inquiry. PTSB reiterated those measures, and its ongoing cooperation, in its submissions of 26 September 2025, in submitting that this should constitute a mitigating factor under this criterion. However, this has separately been taken into account as a mitigating factor under Article 83(2)(c) above.

237. The DPC therefore considers this criterion to be neutral.

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

238. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern Article 9 or 10

[123] EDPB Fining Guidelines, [94].
[124] A29WP Fining Guidelines p14.
[125] EDPB Fining Guidelines, [96].

GDPR data,[126] 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.[127]

239. Due to the absence of the implementation of appropriate technical and organisational measures the categories of personal data not subject to appropriate security and affected by the infringements included mobile phone numbers associated with data subjects' bank accounts, which were used for two factor authentication, bank balances, recent transactions the Open24 numbers assigned by the bank and used for logging in to the Open24 platform. In two cases, this directly led to significant financial loss and put the data subjects at increased risk of additional theft, fraud and financial loss.

240. These personal data, by their nature, carry a high innate risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud. In those circumstances, the DPC considers that the categories of personal data affected by the infringements are an aggravating factor of high weight.

241. In its submission of 26 September 2025, PTSB submitted that the DPC should have regard to the fact that the bad actors were in possession of a certain amount of personal data related to PTSB customers and that this increased the overall risk and impact on the data subjects impacted. While the DPC does not disagree that the prior attacks on data subjects had such an effect, this does not disturb the conclusion that the absence of the implementation of appropriate technical and organisational measures in the Open24 Contact Centre directly led to the disclosure of financial data and data associated with customer bank accounts (such as the phone number used for two-factor authentication, address and Open24 number), which carries a high innate risk, and ultimately led to financial loss in two cases. The DPC is therefore satisfied that it has appropriately afforded weight to the categories of personal data affected by the infringements under this criterion.

[126] Article 9 GDPR 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. Article 10 GDPR provides that "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects".

[127] 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;

242. 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.'[128]

243. The A29WP Fining Guidelines also note that:

> "*The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement*."[129]

244. In this case, the DPC received notifications of three personal data breaches from PTSB on 26 and 27 May 2022. This was found to be an undue delay and therefore an infringement of Article 33(1) GDPR. However, as this forms the basis for the finding of infringement, the DPC considers this factor neutral in this respect.

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;

245. 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*

[128] A29WP Fining Guidelines p15.
[129] A29WP Fining Guidelines p15.

issued to the same controller or processors 'with regard to the same subject matter'".[130]

246. Corrective powers have not previously been ordered against PTSB with regard to the subject-matter of this Decision. As such, the DPC considers this factor to be neutral.

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

247. Such considerations do not arise in this case.

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.

248. The DPC is of the view that there are no other aggravating or mitigating factors in respect of the infringements of Articles 5(1)(f), 32(1) or 33(1) GDPR.

249. In its submissions on the Draft Decision of 26 September 2025, PTSB summarised a range of factors which it considered mitigating. In so doing, it repeated certain submissions already made and which have been taken into account elsewhere in this Decision. For example, PTSB repeated its earlier positions on the steps taken to secure customer accounts following the Breaches, the refund of funds to the two data subjects that suffered financial loss, the prevention of further malicious activity in relation to the relevant accounts and the improvements to technical and organisational measures following the Breaches. Those factors have already been considered in respect of Article 83(2)(c) GDPR above. PTSB also notes that despite the failing in implementing appropriate technical and organisational measures in the Open24 Contact Centre, only three data subjects were concretely affected and suffered damage. The DPC has considered the number of data subjects affected and the level of damage suffered by them in respect of Article 83(2)(a) GDPR.

250. Finally, PTSB's submissions additionally refer to the nature of the Breaches, which involved malicious actors obtaining customer information prior to contacting PTSB and repeated agent error when dealing with those malicious actors. The particular nature of the Breaches

[130] A29WP Fining Guidelines p15.

has been considered by the DPC throughout the Decision and, as noted in the DPC's consideration of Article 83(2)(d) GDPR above, those factors do not limit the responsibility of PTSB to implement appropriate technical and organisational measures to ensure the security of processing or report data breaches under Article 33(1) GDPR. While the background to the particular Breaches is relevant, the DPC does not consider those factors to be mitigating with regard to the specific infringements detailed in this Decision.

Decisions on whether to impose administrative fines

251. 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.'[131]

252. Taking into account the assessment of the criteria at (a) to (k) above, the DPC has decided to impose administrative fines. The infringements were considered above to be of a moderate seriousness by reference to their nature, gravity and duration in line with Article 83(2)(a) GDPR. This is an aggravating factor, which indicates that a fine should be imposed. Under Article 83(2)(b) GDPR the DPC found that PTSB was negligent to a medium degree with respect to the infringements. In addition, under Article 83(2)(g) GDPR, the infringements affected personal data that, by their nature, carry a high risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud. This is an aggravating factor of a high weight indicating that a fine should be imposed. The DPC considers that the measures adopted by PTSB under Article 83(2)(c) to mitigate the damage to data subjects are mitigating to a moderate degree, but this factor does not negate the need for administrative fines in this Inquiry. The DPC considers that the factors assessed in relation to Articles 83(2)(e), (f), (h), (i), (j) and (k) are neither mitigating nor aggravating.

253. In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance. Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR

[131] EDPB, Binding Decision 1/2023.

acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

> "*In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine*."

254. In light of the seriousness of the infringements, the DPC considers that administrative fines are proportionate to dissuade PTSB and other entities from non-compliance with the infringed provisions. The DPC finds that administrative fines are necessary to deter other future serious non-compliance on the part of PTSB and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

    a. Each infringement is moderate in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements of this nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

    b. Regarding the infringements of Articles 5(1)(f) and 32(1) GDPR, the DPC considers that PTSB's non-compliance with its obligations under these Articles must be strongly dissuaded. PTSB's failure to implement appropriate technical and organisational measures was a critical factor contributing to the loss of control of users' personal data and exposure of the data subjects to the risks of theft, fraud or financial loss. Given that such activities constituted a high risk to the rights and freedoms of natural persons the DPC considers that an administrative fine is appropriate and necessary in order to dissuade non-compliance. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. The DPC also considers an infringement of the '*integrity and confidentiality*' principle under Article 5(1)(f) to be particularly serious and this is reflected by the higher fine threshold under Article 83(5) GDPR.

    c. Considering the nature of PTSB's infringements of Articles 33(1) GDPR, and the repetitive nature of those infringements, the DPC considers that imposing an administrative fine for these infringements is necessary to dissuade future non-

compliance on PTSB's part. The reporting and notification requirements under the GDPR do not only serve to protect data subjects' right but also facilitate the efficient exercise of supervisory authorities' investigative and regulatory functions. The exercise of such functions supports the GDPR's aims of protecting data subjects' fundamental rights and the DPC considers it necessary to impose an administrative fine to deter future non-compliance with this provision.

Therefore, the DPC considers that administrative fines are appropriate and necessary in order to dissuade non-compliance.

255. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate for ensuring compliance. PTSB's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the Breaches. In light of this damage, the DPC considers that administrative fines are proportionate in response to PTSB's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR with a view to ensuring future compliance. The DPC considers that the administrative fines imposed do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

256. The DPC considers that the negligent character of PTSB's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to ensure that PTSB directs sufficient attention to its obligations under Articles 5(1)(f), 32(1) and 33(1) GDPR in the future.

257. The DPC considers that administrative fines would help to ensure that PTSB and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

258. The DPC has had regard to the lack of previous relevant infringements by PTSB and has also had regard to the actions taken by PTSB as a result of the Breaches. However, in light of the factors outlined above, the DPC considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

b) Decision on the amount of the administrative fines

259. Above, it was determined that it was necessary to impose administrative fines. This section calculates the amount of those fines, 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

260. 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*."

261. As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. all of the processing operations that PTSB carries out on personal data in the context of its Open24 Contact Centre.

262. 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.[132] In summary, the view of the EDPB is that the correct approach to the interpretation of Article 83(3) GDPR requires that:

> "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*."

263. The impact of this interpretation is that administrative fines are imposed cumulatively, as opposed to imposing only the fine for the gravest infringement. Under this interpretation, the only applicable limit for the total fine imposed is the overall 'cap'. By way of example, in a case of multiple infringements, if the gravest infringement was one that 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.

---

[132] Inquiry IN-18-12-2.

264. In this case, infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR were identified. The gravest infringement is that of Article 5(1)(f), as it is an infringement of a core principle of the GDPR. The associated maximum possible fine for this infringement under Article 83(5) GDPR is €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

ii) Categorisation of the infringements

265. Articles 83(4)-(6) GDPR set out the caps that apply under the GDPR. The EDPB Fining Guidelines say that the categorisation of infringements under Article 83(4)-(6) GDPR can be used to determine the starting point for further calculation. Those 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*."

266. Infringements of Articles 32(1) and 33(1) are subject to a cap under the GDPR of €10,000,000 or 2% of an undertaking's annual turnover, whichever is higher, under Article 83(4) GDPR. However, an infringement of Article 5(1)(f) is subject to a cap of €20,000,000 or 4% of an undertaking's annual turnover, whichever is higher, under Article 83(5) GDPR.

267. 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.

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

268. 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.[133] These factors were assessed in paragraphs 178 to 219 and 238 to 241 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*

[133] EDPB Fining Guidelines, [51].

interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole."[134]

269. Having regard to these factors as a whole, the infringements are of a medium level of seriousness. Under Article 83(2)(a) GDPR the infringements were found to be of a moderate nature and gravity. The infringements of Article 5(1)(f) and 32(1) GDPR were also found to have been of considerable duration. The infringements affected personal data which, by their nature, carry a high risk with regard to the fundamental rights and freedoms of data subjects, as assessed under Article 83(2)(g) GDPR. PTSB was also negligent to a medium degree with respect to the infringements, as assessed under Article 83(2)(b) GDPR. Therefore, balancing these factors, the DPC considers that the infringements were of medium seriousness.

270. As the infringements are of a medium level of seriousness the starting point for calculation is between 10 and 20% of the applicable maximums identified above at paragraph 264.

iv) Turnover of the undertaking with a view to imposing an effective, dissuasive and proportionate fine

271. Citing binding decision 1/2021, the EDPB Fining Guidelines state that the EDPB 'considers that it is fair to reflect a distinction of the size of the undertaking in the starting points identified below and therefore takes into account its turnover.'[135] This view is rooted in Article 83(1) GDPR, which requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also state that this does not 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[136] Article 83(1) will be considered again at the end of this calculation.

272. The EDPB Fining Guidelines state that the supervisory authority may adjust the starting amount corresponding to the seriousness of the infringement by reference to the turnover of the undertaking.[137]

- **For undertakings with an annual turnover of ≤ €2m**, supervisory authorities may

[134] EDPB Fining Guidelines, [59].
[135] EDPB Fining Guidelines, [64].
[136] EDPB Fining Guidelines, [64].
[137] EDPB Fining Guidelines, [64]-[66].

consider to proceed calculations on the basis of a sum between 0.2% and 0.4% of the identified starting amount.[138]

- **For undertakings with an annual turnover of €2m up until €10m**, supervisory authorities may consider to proceed calculations on the basis of a sum between 0.3% and 2% of the identified starting amount.[139]
- **For undertakings with an annual turnover of €10m up until €50m**, supervisory authorities may consider to proceed calculations on the basis of a sum between 1.5% and 10% of the identified starting amount.[140]
- **For undertakings with an annual turnover of €50m up until €100m**, supervisory authorities may consider to proceed calculations on the basis of a sum between 8% and 20% of the identified starting amount.[141]
- **For undertakings with an annual turnover of €100m up until €250m**, supervisory authorities may consider to proceed calculations on the basis of a sum between 15% and 50 % of the identified starting amount.[142]
- **For undertakings with an annual turnover of €250m up until €500m**, supervisory authorities may consider to proceed calculations on the basis of a sum between 40% and 100% of the identified starting amount.[143]
- **For undertakings with an annual turnover above €500m**, supervisory authorities may consider to proceed without an adjustment of the identified starting amount. Indeed, such undertakings will exceed the static legal maximum and, thus, the size of the undertaking is already reflected in the dynamic legal maximum used to determine the starting amount for further calculation based on the evaluation of the seriousness of the infringement.[144]

273. As noted in section (vi) below, according to the PTSB Annual Report for 2024 (the most recent published at the time of this Decision), the total income of Permanent TSB Group

[138] EDPB Fining Guidelines, [65].
[139] EDPB Fining Guidelines, [65].
[140] EDPB Fining Guidelines, [65].
[141] EDPB Fining Guidelines, [66].
[142] EDPB Fining Guidelines, [66].
[143] EDPB Fining Guidelines, [66].
[144] EDPB Fining Guidelines, [66].

Holdings plc in that year was approximately €672,000,000.[145] No adjustment to the starting point is therefore necessary.

274. As noted in the EDPB Fining Guidelines,

> "[I]*t should be reiterated that the starting points for further calculation are not fixed amounts (price tags) for infringements of provisions of the GDPR. The supervisory authority has the discretion to utilise the full fining range from any amount until the legal maximum, ensuring that the fine is tailored to the circumstances of the case*."[146]

v) Aggravating and mitigating circumstances

275. 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,[147] this section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR.

276. In relation to Article 83(2)(c) GDPR, it was noted that PTSB had adopted significant measures to mitigate the damage to data subjects. PTSB promptly made a number of substantial technical and organisational changes as a result of the Breaches and also reimbursed the data subjects who suffered financial loss. This is considered to be a mitigating factor of moderate weight.

277. In relation to Article 83(2)(d) GDPR, it was noted that PTSB did not do 'what it could be expected to do' in the circumstances assessed in this Decision. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 32 GDPR against PTSB, this factor cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

---

[145] PTSB Annual Report 2024. Net Interest Income of €612M + Net Fees and Commissions Income of €55M + Net Other Income of €5M = a total of €672M. The DPC further notes that this figure corresponds to the turnover figure disclosed by PTSB pursuant to its country-by-country reporting requirements, as per the Capital Requirements Directive (CRD IV), as transposed into Irish legislation by Regulation 77 of Statutory Instrument 158 of 2014. As detailed in the latest of those disclosures (2023), the turnover figure comprises "*net interest income, net fees and commission income, net trading income, net other operating income*."

[146] EDPB Fining Guidelines, [69].

[147] EDPB Fining Guidelines, [70].

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

279. In relation to Article 83(2)(f) GDPR, it was noted that PTSB had cooperated with the DPC. As PTSB has a general obligation to cooperate under Article 31 GDPR, this factor is considered to be neither mitigating nor aggravating.

280. In relation to Article 83(2)(h) GDPR, it was noted that the manner in which the infringement became known to the DPC was via notification of personal data breaches from PTSB. The DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

281. In relation to Article 83(2)(i) GDPR, it was noted that orders had not been previously ordered by the DPC[148] with regard to the same subject matter. This factor is considered to be neither mitigating nor aggravating.

282. In relation to Article 83(2)(j) GDPR, 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.

283. In relation to Article 83(2)(k) GDPR, it was noted that there were no additional aggravating or mitigating factors for consideration.

284. 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) GDPR together with the requirements of the Fining Guidelines, as detailed above, the DPC imposes, in respect of PTSB's infringement of Article 5(1)(f) and 32(1) GDPR, a fine of €250,000.

285. In respect of PTSB's infringement of Article 33(1) GDPR, the DPC imposes a fine of €27,500.

286. These fines, totalling €277,500, are substantially lower than the total maximum fine of €385,000 proposed in the Draft Decision. The final fines reflect the mitigation occasioned by PTSB in acknowledging flaws in its technical and organisations measures, indicating its commitment to compliance and protecting data protection rights and promptly making significant improvements in order to reduce the likelihood of similar breaches occurring in the future.

[148] 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.'

vi) The relevant legal maximums for the different processing operations

The relevant undertaking for the purposes of the fine calculation

287. In order to ensure that the fine does not exceed the fining cap and to identify the turnover for the purposes of section (iv) it is first necessary to consider whether or not the fine is to be imposed on "*an undertaking*." Recital 150 clarifies, in this regard, that:

> "*Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes*."

288. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires the DPC to do so by reference to the concept of "*undertaking*," as that term is understood in a competition law context. In this regard, the Court of Justice of the European Union (the '**CJEU'**) has established that "*an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed*".[149]

289. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement.[150]

290. In the context of Article 83 GDPR, the concept of *"undertaking"* means that, where there is another entity that is in a position to exercise decisive influence over the controller/processor's behaviour on the market, then they will together constitute a single

[149] Case C-41/90, *Höfner and Elser v Macrotron GmbH*, Judgment of 23 April 1991, [21].
[150] Case c-97/08P *Akzo Nobel and Others v Commission*, Judgment of 10 September 2009, [58 – 60].

economic entity and a single undertaking. Accordingly, the relevant fining cap will be calculated by reference to the turnover of the undertaking as a whole, rather than the turnover of the controller or processor concerned.

291. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case.[151]

292. The CJEU has established that,[152] where a parent company has a 100% shareholding in a subsidiary, it follows that the parent company is able to exercise decisive influence over the conduct of the subsidiary and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary. The CJEU also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[153]

293. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise decisive influence over the conduct of its subsidiary.[154] This reflects the position that:

> "*…the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day*

[151] C-490/15 P *Ori Martin and SLM v Commission* (14 September 2016) ECLI:EU:C:2016:678, [60].
[152] Case C-97/08 P *Akzo Nobel and Others v Commission* (10 September 2009) EU:C:2009:536.
[153] Case C-508/11 *P Eni v Commission* (8 May 2013) EU:C:2013:289, at para. 48.
[154] T-206/06 *Total and Elf Aquitaine v Commission* (7 June 2011) EU:T:2011:250, at para. 56; T-562/08 *Repsol Lubricantes y Especialidades and Others v Commission* (12 December 2014) EU:T:2014:1078, at para. 42; T-413/10 and T-414/10 *Socitrel and Companhia Previdente v Commission* (15 July 2015) EU:T:2015:500, at para. 204.

business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company…"[155]

294. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and legal links between the two entities, that the subsidiary acts independently on the market. It is important to note that *"decisive influence"*, in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

295. In Permanent TSB Group Holdings plc's Annual Report of 2024,[156] it is stated that "*Permanent TSB plc (PTSB), a 100% owned subsidiary of the Company, is the main trading entity of the Group which is involved in retail banking*."

296. Therefore, as the "ultimate parent company" it is assumed that Permanent TSB Group Holdings plc is in a similar situation to that of a sole owner as regards its power to (directly or indirectly) exercise a decisive influence over the conduct of PTSB. Accordingly, a rebuttable presumption arises to the effect that Permanent TSB Group Holdings plc does in fact exercise a decisive influence over the conduct of PTSB on the market. If this presumption is not rebutted, it would mean that PTSB and Permanent TSB Group Holdings plc constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant cap for the purpose of Articles 83(5) GDPR would fall to be determined by reference to the total turnover of all of the component companies in the undertaking, namely PTSB and Permanent TSB Group Holdings plc. According to the PTSB Annual Report for 2024 (the most recent published at

[155] Case C-97/08 P *Akzo Nobel and Others v Commission* EU:C:2009:262 (Opinion of Advocate General Kokott), at para. 73 cited in Case T-419/14 *The Goldman Sachs Group, Inc. v European Commission* (12 July 2018) ECLI:EU:T:2018:445, at para. 51.

[156] Permanent TSB Group Holdings plc, Annual Report 2024, (*Permanent TSB Group*, 3 March 2025) < https://www.permanenttsbgroup.ie/~/media/Files/P/Ptsb-CORP/documents/result-centre/annual-interim/2024/ptsbgh-annual-report-2024.pdf >, last accessed: 12 May 2025.

the time of this Decision), the amount of that turnover in this year was approximately €672,000,000.[157]

297. On 1 August 2025, the DPC wrote to PTSB setting out the concept of undertaking and how it applies in the context of the GDPR and detailing the DPC's understanding of the relevant factors, as they appear to apply to PTSB.

298. On 14 August 2025, PTSB responded to the DPC and confirmed that Permanent TSB Group Holdings plc and PTSB constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. PTSB further confirmed that it had brought the contents of the DPC's letter dated 1 August 2025 to the attention of the relevant members of Permanent TSB Group Holdings plc who had no further observations to make arising out of the DPC's letter.

299. As the presumption was not rebutted, but rather confirmed by PTSB, it means that PTSB plc and Permanent TSB Group Holdings plc constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant cap for the purpose of Articles 83(4) and (5) GDPR, falls to be determined by reference to the combined turnover of PTSB and Permanent TSB Group Holdings plc.

300. According to the EDPB Fining Guidelines:

> "*Turnover is taken from the annual accounts of an undertaking, which are drawn up with reference to its business year and provide an overview of the past financial year of a company or of a group of companies (consolidated accounts). Turnover is defined as the sum of all goods and services sold. Net turnover means the amount derived from the sale of products and the provision of services after deducting sales rebates*

[157] PTSB Annual Report 2024. Net Interest Income of €612M + Net Fees and Commissions Income of €55M +Net Other Income of €5M = a total of €672M. The DPC further notes that this figure corresponds to the turnover figure disclosed by PTSB pursuant to its country-by-country reporting requirements, as per the Capital Requirements Directive (CRD IV), as transposed into Irish legislation by Regulation 77 of Statutory Instrument 158 of 2014. As detailed in the latest of those disclosures (2023), the turnover figure comprises "*net interest income, net fees and commission income, net trading income, net other operating income.*"

and value added tax (VAT) and other taxes directly linked to turnover.[158]

Turnover is taken from the presentation of the profit and loss account.[159] *Net turnover includes revenue from the sale, rental and leasing of products and revenue from the sale of services less sales deductions (e.g. rebates, discounts) and VAT."*[160]

301. The relevant turnover for the purposes of Article 83(4)-(6) GDPR is the turnover for the preceding financial year. The EDPB Fining Guidelines State:

> "*As to the question of which event the term "preceding" relates to, the CJEU case law in competition law is also to be applied for GDPR fines so that the relevant event is the fining decision issued by the supervisory authority and neither the time of infringement nor the court decision*."[161]

302. With regard to the relevant year for the calculation of turnover, in its correspondence of 14 August 2025, PTSB stated that it was of the view that "*consideration should be given to using the financial year 2021 as the relevant financial year (i.e. the year preceding the incidents which gave rise of the alleged data breaches the subject of the Inquiry), rather than 2024, in circumstances where the Inquiry has been ongoing for nearly three years*". However, as noted by the EDPB in Binding Decision 1/2021, the date of the final decision taken by the Lead Supervisory Authority is the event from which the preceding financial year should be considered.[162] Although Binding Decision 1/2021 referred to an inquiry where cross-border data processing was at issue, the DPC does not consider that there is any reason to depart from the view of the EDPB in relation to an inquiry where domestic

---

[158] Footnote from EDPB Fining Guidelines: *See e.g., Article 2(5) of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (hereinafter "Directive 2013/34/EU"), which is applicable to companies with limited liability, or similar applicable legislation and Article 5(1) of Council Regulation (EC) No. 139/2004 on the control of concentrations between undertakings (hereinafter "EC Merger Regulation").*

[159] Footnote from EDPB Fining Guidelines: *See e.g., Annexes V or VI to Article 13(1) of Directive 2013/34/EU under the heading "net turnover", or similar applicable legislation.*

[160] EDPB Fining Guidelines, [128]-[129].

[161] EDPB Fining Guidelines, [131]. This paragraph of the EDPB Fining Guidelines has the following footnote: Regional Court LG Bonn, case 29 OWi 1/20, 11 November 2020, paragraph95, referencing case C-637/13 P, Badezimmerkartell Laufen Austria, para. 49 and case C-408/12 P, YKK et al, para. 90.

[162] Binding decision 1/2021 on the dispute arisen on the Draft Decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted on 28 July 2021.

data processing is at issue. The DPC therefore uses the best available and most up to date financial information in making this calculation.

303. Above, it was determined that the infringement of Article 5(1)(f) GDPR was the gravest infringement. Therefore, the cap for the fines in this decision is 4% of the undertaking's total worldwide annual turnover of the preceding financial year. The DPC notes that the imposed fines are cumulatively less than 4% of Permanent TSB Group Holdings plc worldwide annual turnover from the most recently published annual accounts.

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

Effectiveness

304. 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. The infringements concern personal data including data subject identity, contact details, and economic or financial data. These personal data, by their nature, carry a high risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud. In that context, the DPC considers that the level of the imposed fines is sufficient to ensure compliance and no further adjustment is required.

Dissuasiveness

305. 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 imposed ranges are dissuasive for both. The DPC considers the monetary value of the imposed fines to be sufficient to have such a deterrent effect.

306. Each infringement is moderate in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a moderate nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Regarding the infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR, the DPC considers that PTSB's non-compliance with its obligations under these Articles

must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, the DPC considers that the imposed administrative fines are appropriate and necessary in order to dissuade non-compliance.

307. The DPC considers that the negligent character of PTSB's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR carries weight when considering the amount of those fines. This negligence suggests that the imposed administrative fines are necessary to ensure that PTSB directs sufficient attention to its obligations under Articles 5(1)(f), 32(1) and 33(1) GDPR in the future.

308. The DPC considers that the imposed amounts of the administrative fines would help to ensure that PTSB and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

309. The DPC has had regard to actions taken by PTSB as a result of the Breaches. In light of the negligent character of the infringements, and PTSB's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines to the extent imposed are necessary in the circumstances to ensure future compliance.

Proportionality

310. 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 PTSB'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 imposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

311. Having regard to the nature, gravity and duration of the infringements, the DPC considers that the imposed administrative fines are proportionate in the circumstances in view of ensuring compliance. In particular, PTSB's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the Breaches, which led to financial loss and loss of control over personal data for data subjects, who were put at increased risk of additional theft, fraud, or financial loss. The lack of appropriate technical and organisational measures additionally meant other PTSB customers were vulnerable to similar damage occurring. In light of this damage, the DPC considers that the imposed administrative fines are proportionate to respond to PTSB's infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR with a view to

ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

M. Summary of Envisaged Action

312. In summary, the corrective powers that the DPC imposes to address the infringements in the particular circumstances are:

- A Reprimand to PTSB pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision;
- One imposed administrative fine for infringement of Articles 5(1)(f) and 32(1) GDPR in the amount of €250,000; and
- One imposed administrative fine for the infringement of Article 33(1) GDPR in the amount of €27,500.

N. Right of Appeal

313. The Final Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, PTSB has the right to appeal against the Final Decision within 28 days from the date on which notice of the Final Decision is received by it. Furthermore, pursuant to section 142 of the 2018 Act, as the Final Decision includes a Decision to impose an administrative fine, PTSB also has the right to appeal against that Decision within 28 days from the date on which notice of the Final Decision is given to it.

<u>This Decision is addressed to:</u>
Permanent TSB plc,
56-59 Stephen's Green,
Dublin 2,
D02 5489

Decision-Makers for the Data Protection Commission:

_____
Dr. Des Hogan
Commissioner for Data Protection
Chairperson

_____
Dale Sunderland
Commissioner for Data Protection

An Coimisiún um Chosaint Sonraí
Data Protection Commission

APPENDIX 1

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]

An Coimisiún um Chosaint Sonraí
Data Protection Commission

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

An Coimisiún um Chosaint Sonraí
Data Protection Commission

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

An Coimisiún um Chosaint Sonraí
Data Protection Commission

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]