In the matter of the General Data Protection Regulation

Commission Case Reference: IN-20-7-2

In the matter of Bank of Ireland Group plc

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

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

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

27 February 2023

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. Introduction

1. This document (**'the Decision'**) is a decision made by the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**). I make this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act. A member of the inquiry team of the DPC (**'the Case Officer'**) provided Bank of Ireland Group plc (**'BOI'**) with an Inquiry Issues Paper in order to make submissions on it.

2. BOI was provided with the draft decision in this Inquiry on 25 November 2022 (the "**Draft Decision**") to provide it with a final opportunity to make submissions. BOI made submissions on the Draft Decision on 21 December 2022. I have given full consideration to these submissions in finalising this Decision. This Decision is being provided to BOI pursuant to Section 116(1)(a) of the 2018 Act in order to give BOI notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

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

B. Legal Framework for the Inquiry and the Decision

i) Legal Basis for the Inquiry

4. 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 on foot of a complaint, or of its own volition.

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

ii) Data Controller

6. In commencing the Inquiry, the DPC considered that BOI may be the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that was the subject of the personal

data breach notifications. In this regard, BOI confirmed that it was the controller in its notification of ten personal data breaches to the DPC between 30 January 2020 and 6 May 2020.[1]

iii) Legal Basis for the Decision

7. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry and any other materials which I consider to be relevant, in the course of the decision-making process.

8. The Inquiry Issues Paper was finalised on 26 July 2021. BOI made submissions on the Inquiry Issues Paper on 17 August 2021. A full schedule of all documentation considered by me for the purpose of the preparation of this Decision is appended hereto.

9. Having considered the information obtained in the Inquiry, I am satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. The DPC has had regard to any submissions that BOI made in respect of the Draft Decision before proceeding to make this Final Decision under section 111 of the 2018 Act.

C. Factual Background

10. BOI provides online and phone banking services via its Banking365 service ('Banking365'). The associated terms and conditions of the Banking365 service state that the '365 online' service is defined as the internet banking service accessed via a web browser.[2]

11. The DPC received ten personal data breach notifications from BOI between 30 January 2020 and 6 May 2020. The data breach notifications concerned the unauthorised access to and disclosure of personal data processed within the Banking 365 platform. In six of the ten data breaches, unauthorised persons gained access to customers' accounts online as a result of staff not following BOI procedures correctly.[3] The remaining four data breaches, in which unauthorised people gained access to customers' accounts online, were as a result of a flaw in the Customer Information System ('CIS'). BOI was made aware of a number of cases where customers who logged into their unique account through the Banking365 portal could view the account transaction details of third parties.[4]

12. The DPC issued an Inquiry Commencement Letter ('the Commencement Letter') by email and registered post to BOI on 12 August 2020[5] notifying the company that the DPC had

[1] Appendix C.2 Breach Notifications With Correspondence
[2] Appendix C.4.18 365 Online Terms and Conditions Section 1.1 "Definitions" page 1
[3] Appendix C.4.2 pages 16-18
[4] Appendix C.2 Breach Notifications With Correspondence
[5] Appendix C.3 Commencement Letter

commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act. The letter contained details of the personal data breaches notified to the DPC which would be the subject of the Inquiry and it contained seven questions seeking further information from BOI.

13. The decision to commence the Inquiry was taken having regard to the circumstances of personal data breaches notified by BOI. The Commencement Letter informed BOI that the Inquiry would examine whether or not BOI discharged its obligations in connection with the subject matter of the personal data breaches and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by BOI in that context. In this regard, the scope of the Inquiry was expressly stated to include the steps taken by BOI to comply with the principle of integrity and confidentiality pursuant to Article 32(1) GDPR among other Articles.

14. The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The relevant facts ascertained during the personal data breach notification and handling process were set out in the Commencement Letter. The facts, established during the course of the Inquiry, are set out below in this Decision.

15. BOI provided submissions in response to the Commencement Letter on 9 September 2020. In its submissions, BOI outlined the technical and organisational measures which BOI had in place to meet the requirements of the GDPR. The submissions outlined policies and procedures, staff training and quality assurance sampling in relation to data protection governance.[6]

16. The submissions also outlined the steps that BOI has taken since the personal data breaches in order to comply with the GDPR including details of organisational and technical measures. The submissions appended a number of documents, which are considered throughout this Decision.

17. On 8 April 2021, the Case Officer requested additional documentation related to the BOI Banking Service Desk Procedures, Customer Verification procedures and Customer Confidentiality Service Standards, as well as further information relating to accounts merging issues.[7] BOI provided submissions in response on 29 April 2021.[8]

18. Having received BOI's submissions, the DPC prepared an Inquiry Issues Paper to document the relevant facts established and the issues that fell for consideration by me as Decision-Maker for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry. The Case Officer furnished BOI with the Inquiry Issues Paper on 26 July 2021[9] and invited BOI's submissions on any inaccuracies and/or incompleteness in the facts.

19. BOI provided comments on the Inquiry Issues Paper on 17 August 2021.[10] The comments included some textual amendments and supplemental information relating to the facts as set out in the Inquiry Issues Paper. BOI's comments were analysed and the DPC has considered

[6] Appendix C.4 Submissions 9 September 2020
[7] Appendix C.5 Commission Queries 8 April 2021
[8] Appendix C.6 Submissions 29 April 2021
[9] Appendix C.7 Issues Paper
[10] Appendix C.8 Submissions 17 August 2021

them as part of this Decision.The data breach notifications concerned the unauthorised access to and disclosure of personal data processed within the BOI Banking 365 ('Banking365') platform. BOI were made aware of a number of cases where customers were able to log into their unique Banking365 portal and view the details of third parties.

20. Six of the ten data breaches were as a result of staff not following BOI procedures correctly. The remaining four data breaches were as a result of incorrect merging of customer accounts due to the Nine Year Algorithm in BOI's Customer Information System (CIS). For some of the 10 breaches, someone who was not the account holder was given full access to the BOI365 services, e.g. BN-20-2-110, BN-20-3-678, BN-20-4-12, BN-20-4-268, BN-20-4-350. Other breaches amounted to unauthorised access/disclosure giving a view of the account transactions to an unauthorised third party, e.g. BN-20-3-418, BN-20-4-429, BN-20-4-425 while BN-20-5-107 involved an unauthorised view of credit card details and BN-20-4-270 involved both unauthorised access and unauthorised disclosure.

21. I am obliged to consider all of the information obtained in the Inquiry and to reach conclusions as to whether I identify infringements of data protection legislation. The Inquiry Issues Paper sets out the factual background and the scope and legal basis for the Inquiry. As set out above in Section A, this document is the Decision on this matter and it includes the corrective powers that will be exercised arising from the infringements that are identified herein.

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

22. The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not BOI 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 BOI in that context.

23. In this regard, the Commencement Letter specified that the Inquiry would focus on BOI's organisational and technical measures in place to ensure security of the personal data. In particular, the Commencement Letter expressly stated that the scope of the Inquiry would include Articles 5(1)(f) and 32(1) GDPR. The Commencement Letter stated that the Inquiry would focus on the areas of Data Protection Governance, Training and Awareness, Records Management and Security of Personal Data.

24. The material scope of the GDPR under Article 2 applies to processing of personal data. The financial data of customers that is processed in the course of the Banking 365 service meets the definition for personal data under Article 4(1) GDPR.

E. Submissions in relation to the Draft Decision

25. The Draft Decision was provided to BOI on 25 November 2022, and BOI was requested to furnish any submissions it wished to make to the DPC. BOI furnished its submissions in respect of the Draft Decision on 21 December 2022 ('**BOI Submission 21 Dec 2022**'). BOI stated that its submissions were in respect of the following areas: risk; methodology for assessment;

likelihood of risk; severity of risk; testing, training and quality assurance; categorisation of BOI's actions as 'negligent'; remedial actions; drafting and clarification points; and redaction.

26. I have given full consideration to BOI's submissions in relation to the above mentioned points.

27. BOI also states that the "*volume of data subjects using a particular access method does not automatically increase the risks of processing activity using that method.*" However, the DPC position is that the more data subjects using a service, the more adverse impact there may be if a breach materialises as it may affect large numbers of users.The DPC agrees with BOI that other factors need to be taken into consideration, apart from the number of users but the DPC disagrees it follows from this that the risk is low. High risk is also assessed by reference to the type of personal data concerned and the context of the processing. In the context of this inquiry, the data in customer accounts are very sensitive.

F. Issues for Determination

28. Having reviewed the Issues Paper and the other relevant materials, I consider that the key issue in which I must make a decision is whether BOI has infringed Articles 5(1)(f) and 32 GDPR in respect of its processing of personal data via the Banking 365 Service.

G. Articles 5(1)(f) and 32 GDPR

29. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires 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.*

30. Article 32(1) GDPR provides:

> *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.*

31. In considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.

32. 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.*

a) Assessment of the Risks

33. The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the processing. Regarding BOI's processing of personal data on the Banking 365 platform, those risks include the risk of unauthorised access and unauthorised disclosure of personal data to third parties of personal data processed within the platform.

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

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

35. 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 the Banking365 process must consider, first, the likelihood of unauthorised access to, or disclosure of, customers' accounts online, 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.

36. The key risk arising from this processing of customers' personal data on the Banking365 app was that an unauthorised person would gain access to a customer's account and/or be able to use any or all of the elements of the service listed below. This would result in a high risk of fraud and/or identity theft. BOI states "*there has never been an instance of fraud or identity theft arising from these types of events*"[11] and therefore, "*it appears that the risk of fraud and/or identity theft is a potential harm*".[12] However, the fact that a risk has not yet materialised as a harm, as far as BOI is aware, does not reduce the severity of the risk itself.

[11] Appendix C.9.1 BOI Submission 21 Dec 2022, page 5
[12] Appendix C.9.1 BOI Submission 21 Dec 2022, page 5

In fact, risk is not gauged after the event, but rather by reference to conditions before the risk event materialised.

37. The risks of fraud and identity theft would severely undermine a customer's relationship with the bank as the relationship is premised on the agreement the bank will 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.

38. In addition, the Banking365 app was offered as an access method for the majority of the customer base and therefore, any breach that would occur would have potential adverse impacts across a large user base.

39. Regarding how BOI evaluated the risk arising in respect of the security of personal data and, in particular, the risk arising from how BOI provided access to the Banking 365 platform, BOI stated that

> *Bank of Ireland ('the Bank') manages its exposure to a multitude of risks which arise in the course of its business (including data protection and information security) in line with the Bank's Risk Management Framework. This Risk Management Framework outlines the expectations of Business Units within the Bank when managing risk, including any associated elements such as data breaches and technical/organisational control measures.*[13]

40. BOI also stated that

> *Risks and controls are subject to cyclical reviews, the frequency of which is dependent on the severity and likelihood of the risk. Changes in processes or the introduction of new services may also give rise to a risk rating review.*[14]

41. BOI processes a vast quantity of personal data on the Banking 365 platform in respect of a significant number of data subjects. The personal data processed by BOI via Banking 365 includes, among other things, customers' account balance, information about transactions, setting up or viewing standing orders, funds transfer and payments to other designated accounts, bill payment and requesting account statements for current, savings and loan accounts.

42. The purpose of the processing was determined by BOI in order to enhance customer experience. The key elements of the service provided by Banking365 include enabling customers to access 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 BOI accounts, view recent credit card transactions, customise current account transaction history on screen, show policy details, along with any additional services outlined in future terms and conditions and any other or future services that BOI may develop or introduce.[15] The potential risks

[13] Appendix C.4.2 page 1
[14] Appendix C.4.2 page 1
[15] Appendix C.4.18 at 1.37 page 3

associated with unauthorised persons being able to access and use another user's account include identity theft, fraud and financial loss.[16]

43. I find that BOI's processing of personal data on the Banking 365 platform creates a high risk to the rights and freedoms of natural persons in terms of severity. I acknowledge BOI's submissions that their assessment of the risk was low for the following reasons - the problems being swiftly remediated on BOI's part, there not being a deliberate attempt at fraud and *"there is often a connection between the individuals involved (e.g. same name, familial relationship)."*[17] However, the risk of identity theft, fraud, financial loss and other potential harm pertained in every case. I have also considered BOI's submission that *"the likelihood of the risk of the issue arising is low by reference to the size of the customer base"*[18] I do not accept this point particularly in light of the 9 year algorithm and the potential for over-merging of accounts. I therefore find the likelihood to be moderate in those circumstances.

Security Measures Implemented by BOI

44. BOI's submissions outlined the technical and organisational measures that it had in place at the time of the personal data breaches in order to ensure the ongoing confidentiality and integrity of the processing of personal data on the Banking 365 platform. These measures can be categorised within the areas of scope specified in the Commencement letter as follows:

a) Data protection governance
b) Training and awareness
c) Records management
d) Security of personal data

(a) Data protection governance

45. BOI outlined that it had a range of policies and procedures in relation to data protection including the following operating procedures-

- Banking Service Desk Procedures[19]
- The Business Operating Procedures - Account Conversion Procedure[20]
- Customer Confidentiality/Verification[21]
- Customer Confidentiality Service Standards[22]

[redacted] Section 6.2.7 of the Banking Service Desk Procedures outlines the steps a staff member should take to *"register an account for a 365 digital channel"*.[23] [redacted]

[16] See Recital 75 GDPR
[17] Appendix C.8.2, page 1-2
[18] Appendix C.9.1 BOI Submission 21 Dec 2022, page 5
[19] Appendix C.4.3
[20] Appendix C.6.2 page 7
[21] Appendix C.6.2 page 10
[22] Appendix C.6.2 page 10
[23] Appendix C.4.3 page 3

[redacted]

47. Section 7.3[24] of the Banking Service Desk Procedure outlines how an adviser can add credit card accounts to the Banking 365 platform. [redacted]

48. In addition, BOI issued a 'Must Read memo' on 9 March 2020 (prior to this breach) reminding staff that

> [redacted] *There are very clear guidelines on ledger title structure in the BOP and these should be followed to the letter...*[25]

(b) Training and Awareness

49. BOI stated that risk event and reporting training was completed by all advisers in October 2019 by way of an audio training module.[26] In this training, the primary theme was how to identify different types of operational risk and what channels staff should use to correctly report those risk events *after* they have arisen. The risk event and reporting training includes only a brief reference to the merging of client account data.[27]

50. BOI also stated that a '*Reducing Errors Webinar and Workbook*' was delivered over four weeks in November-December 2019.[28] This training was designed to highlight the need to reduce manual errors when dealing with customer information; however, the module does not make any specific reference to the GDPR or the Data Protection Act 2018.

51. According to BOI, detailed Service Contact Centre Procedures are provided to staff who work in the customer contact centre. These procedures highlight the steps to be undertaken to ensure Banking 365 Online customers are correctly verified. Following the breaches, refresher training was provided to staff on the relevant procedures in order to reduce the risk of errors occurring. Risk focus memos were also issued to all Branch Network staff, reminding them of the procedures for amending customer data.[29] Data protection training and error related training was provided for advisers working in 'Direct Customer Contact' centres in the twelve months prior to September 2020. BOI also pointed out

> *actions taken to address performance may include refresher training sessions on procedures, retraining, 1:1 coaching, team leader / '1 up' review of activities, informal improvement plans, formal improvement plans or disciplinary sanction.*[30]

---

[24] Appendix C.6.2 page 6
[25] Appendix C.6.2 page 8
[26] Appendix C.4.2 page 8
[27] Appendix C.4.12 page 2
[28] Appendix C.4.7
[29] Appendix C.4.2 page 2
[30] Appendix C.9.1 BOI Submission 21 Dec 2022, page 7

52. BOI submitted further training modules dated March 2020, May 2020, July 2020 and August 2020. Some of these modules, however, post-date the breaches that are the subject of consideration in this inquiry.

53. BOI also stated that

> *In respect of the breaches that form the subject of this Inquiry, no advisor was responsible for more than one manual error.*[31]

and that

> *Feedback was provided to all advisers where non-compliance with procedures was identified, including details of how the error impacted the customer.*[32]

54. With regard to the breach caused by a staff member not adhering to Customer Verification Procedures and Customer Confidentiality Standards, according to BOI:

> *thorough checks were not carried out by staff in relation to the customer.*

(c) Records Management

55. BOI outlined that it had a range of oversight and quality assurance measures in place,[33] including-

- Quality Assurance Frameworks – this is a series of reviews and meetings which are held within the bank on a monthly basis. The purpose of the meetings are to review performance against key performance indicators. The BOI Controls Operating Effectiveness ('**COE**') Team evaluate management information which includes call monitoring. The management information is then delivered to the framework meetings and action plans and remediation procedures are agreed.
- Call Monitoring is completed on a monthly basis. Team leaders review a minimum of one call per agent, per month, and any errors are addressed at a monthly coaching session.
- QA Linking Status – Daily quality assurance reviews on applications where account linking has been requested.
- Defects Tracking – Daily reviews and monitoring of quality assurance activities to ensure that accounts which have been linked incorrectly are remediated in an expedient manner.
- BOI Group Internal Audit review

56. However, according to BOI,

[31] Appendix C.9.1 page 6
[32] Appendix C.9.1 page 6
[33] Appendix C.4.2 pages 12-15

[redacted] *BOI's standard operating procedures are designed to ensure, in as much as possible, no errors in terms of relevant data*[34]

57. BOI indicated that it had a range of records management oversight measures in place to ensure the integrity and security of customers' personal data, including-

- Service Contact Centre Procedures – These are step by step instructions and standard operating procedures which are circulated to all staff. BOI have provided a copy of the procedure associated with adding account or credit card features to the Banking 365 platform.
- Branch Operating Procedures – These are standard operating procedures in place to provide staff guidance on how to process different customer requests, transactions and supporting activities. These procedures are updated regularly and are updated when new processes are introduced or where existing processes are changed.[35]

58. Manual merging of customers' accounts and records should follow the relevant procedures and is verified by a BOI operations team. [redacted][36]

(d) Security of Personal Data

(i) Technical Measures

59. In addition to the policies and procedures noted above, BOI described specific technical measures[37] that it stated were in place at the time of the breach, including:

- QA Linking Status – daily quality assurance reviews on applications where account linking has been requested.
- Defects Tracking – daily reviews and monitoring of quality assurance activities to ensure that accounts which have been linked incorrectly are remediated in an expedient manner.
- Security Certificates

[redacted][38]

This system, however, is entirely reliant on the fact that the recipient device or server is the intended device or computer. If the banking customer is authorised by the bank to view a particular account, then [redacted] their

[34] Appendix C.8.2 page 3
[35] Appendix C.4.2 pages 12-15
[36] Appendix C.4.2 page 2
[37] Appendix C.4.2 pages 12-15
[38] Appendix C.4.2 page 3

device will enable that user to view that particular account – even if that account was not owned by that user.

- BOI uses proprietary software ('[redacted]') which is designed to assess and flag unusual patterns in customer access and payments.[39]

- Security Information and Event Management - (**'SIEM'**) is used for security and event controls and will flag if some suspicious entries are detected in banking logs. If suspicious activity is detected then the software will automatically alert the Bank's IT Team.[40] It is noted that SIEM failed to detect unauthorised access to the bank accounts under consideration, as the accounts had been provisioned incorrectly with access owing to gaps in procedures and human error.

60. In six of the ten data breaches, unauthorised persons gained access to customers' accounts online as a result of staff not following BOI procedures correctly.[41]

61. The remaining four data breaches, in which unauthorised people gained access to customers' accounts online, were as a result of a flaw in the CIS. BOI stated that –

[redacted][42]

62. When the Banking365 platform was launched in the late 1990s, the CIS was the basis for the information utilised by the Banking365 platform.[43] [redacted][44]

The impact of this is access to and potential disclosure of the affected accounts by an unauthorised third party.

63. Also, the customer matching and merging process can cause [redacted] to become 'lost' within CIS which results in a default [redacted] being assigned to the customer record. According to BOI -

[redacted][45]

This, in turn, can result in unintended account merging, the impact of which is access to and potential disclosure of the affected accounts by an unauthorised third party. Article 5(1)(f) GDPR requires that personal data shall be *"processed in a manner that ensures appropriate security of the personal data".*

[39] Appendix C.4.2 page 3
[40] Appendix C.4.2 page 3-4
[41] Appendix C.4.2 pages 16-18
[42] Appendix C.4.2 page 6
[43] Appendix C.4.2 page 6
[44] Appendix C.4.2 page 6
[45] Appendix C.4.2 page 6

64. According to BOI the issue with the CIS

> *was originally identified in 2019, following a BOI Group Internal Audit (GIA) review, which predated the inquiry.*[46]

65. BOI stated that from March 2021 it carried out an analysis of cases where over-merging may have occurred. According to BOI these cases-

> *have been categorised into 3 Priority Cohorts. Priority 1 (349 cases) contain the potential over-merges, Priority 2 (2,222 cases) possible over-merges, Priority 3 (2,007 cases) low possibility over-merges.* [47]

In addition, BOI stated that-

> *A review of all cases, and remediation of all identified over-merges is to complete by the end September. Full closure of the over-merging issue, including customer communications and restitution where required, is expected by end of November 2021.*[48]

BOI stated that-

> *[a]s of 26th February 2021* [redacted] *has been removed and the system now requires an exact* [redacted] *match.*[49]

BOI also stated that it had

> *developed a systemic remediation process to prevent further over-merging occurring in the future.*[50]

(ii) Organisational Measures

66. BOI outlined that it had a range of organisational measures relating to security,[51] including the following-

- Clean Desk Procedures – This outlines the physical measures associated with the management of customer information, and includes measures such as the use of locked cabinets and secure shredding bins.
- Physical Access – These are additional physical security measures which prevent unauthorised access to restricted areas. These measures are reviewed annually.
- Group Code of Conduct – The code encompasses the principles of the Irish Banking Federation Code of Ethics, and sets out acceptable standards for group employees who deal with customers, suppliers, Government representatives or Regulators. A

[46] Appendix C.8.2 page 2
[47] Appendix C.8.2 page 2
[48] Appendix C.8.2. page 3
[49] Appendix C.6.2 page 3
[50] Appendix C.8.2 page 3
[51] Appendix C.4.2 page 13-14

mandatory annual web based training course on the Code of Conduct is undertaken by all staff.

67. BOI also pointed out that over the course of 2021 *"as part of the Bank's Central Credit Register ('CCR') Data Protection Action Plan"*[52] BOI put in place a number of actions including an improved Group Data Management Policy and Standards, an Enhanced Group Data Management Operating Model and a revised Data Protection Event Framework. While the DPC welcomes these improvements and enhancements, they fall outside the temporal scope of this inquiry.

b) The Appropriate Level of Security

(a) Measures to evaluate the effectiveness of data protection governance

68. Article 32(1)(d) GDPR specifies that, where appropriate, the controller shall implement technical and organisational measures to include a process for regularly testing, assessing and evaluating the effectiveness of existing security measures. Such testing, assessing and evaluating applies to both technical and organisational measures. Personal data breaches may cause significant harm to data subjects and, pursuant to Article 32(1)(d) GDPR, controllers must take the initiative to test, assess, and evaluate their organisational and technical security measures.

69. Six of the ten reported data breaches were as a result of staff not following the Banking Service Desk Procedures, of which one was as a result of not following the Business Operating Procedures, and one as a result of not following Customer Verification procedures and Customer Confidentiality Service Standards. However, the procedure extract[53] submitted by BOI does not indicate if there are any additional alerts or controls to prevent human error or an incorrect account from being added.

70. BOI had a range of Data Protection Governance policies and procedures in place to ensure the integrity and security of customers' personal data. However, these policies and procedures did not include additional controls to minimise the possibility of human error occurring. While there were follow-ups on the part of BOI with regard to breaches caused by staff not following policies and procedures, I consider that the checks and enforcement measures in place 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 manually populate user fields to permit users to access their sensitive personal data, such as financial transactions, 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 the staff members give effect to the controller's policies and procedures. I have had regard to BOI's monthly call monitoring whereby Team leaders review a minimum of one call per agent, per month, and that any errors are addressed at a monthly coaching session. I find that this level of testing was not appropriate to the risk. Considering the importance of maintaining the security of customers' accounts and the high

[52] Appendix C.9.1 BOI Submission 21 Dec 2022, page 8
[53] Appendix C.4.3

risks to the customer arising as a result of accounts being compromised, BOI ought to have implemented more robust testing measures. I therefore find BOI infringed Article 5(1)(f) and Article 32 GDPR by failing to implement more robust testing measures.

(b) Effectiveness of Training and Awareness

71. In general, training needs to be frequent, regular and appropriate to the activities being carried out. The sensitivity of the data processed by BOI, the detailed nature of its Service Contact Centre Procedures and the manual population of user fields by staff which permits users to access their sensitive personal data means that training should be provided to staff frequently and in great detail in order to reduce the likelihood of manual errors leading to loss of confidentiality of personal data, as occurred in six of the ten breaches.

72. 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. The unintended merging of customer accounts was identified as a contributing factor in relation to the unauthorised disclosure of account information. This account merging issue was originally identified by BOI in 2019. However, the Risk Event Audio Training module in October 2019, while it did cover data protection breaches and there was specific reference made to the merging of client data, the issue was not explained to staff in detail. I find that the level and frequency of staff training provided was not appropriate to the risk. Considering the importance of maintaining the security of customers' accounts and the high risks to the customer arising as a result of unauthorised disclosure, BOI ought to have implemented more frequent and detailed training provisions and I find BOI infringed Article 5(1)(f) and Article 32(1) by failing to do so.

Records Management

73. BOI had a range of Data Protection Governance policies and procedures in place to ensure the integrity and security of customers' personal data. However, these policies and procedures did not include additional controls to prevent human error. While there were follow-ups on the part of BOI with regard to breaches caused by staff not following policies and procedures, I consider that the checks and enforcement measures in place 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 manually populate user fields to permit users to access their sensitive personal data, such as financial transactions, 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 the staff members give effect to the controller's policies and procedures. I have had regard to BOI's monthly call monitoring whereby Team leaders review a minimum of one call per agent, per month, and that any errors are addressed at a monthly coaching session. I find that this level of testing was not appropriate to the risk and that it infringed Article 5(1)(f) and Article 32(1) GDPR by failing to implement adequate testing.

(c) Technical Measures

(i) Testing Security of Personal Data

74. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires that personal data shall be *"processed in a manner that ensures appropriate security of the personal data."* An appropriate level of security includes **technical measures** that have, *inter alia*, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as Article 32(1)(b) provides. The issues with the CIS, [redacted], introduced a risk of over-merging of customer accounts and thus, allowing unauthorised access to customers' financial data. BOI first identified the over merging issue in July 2019 and took steps to analyse potential invalidly merged accounts from March 2021 onwards, and where appropriate, to rectify them. This rectification could have been implemented in a more timely fashion in response to the risks first identified by BOI's internal GIA audit in July 2019, which is prior to the occurrence of the personal data breaches examined in this inquiry. There was a twenty one month gap between BOI identifying the over merging issue on the CIS, via its internal audit in 2019, and providing a final technical fix.

75. Upon becoming aware of the issue of account merging, BOI did not take immediate effective steps to prevent ongoing data breaches that arose from the same issue. BOI points out that it has

> *developed a systemic remediation process to prevent over-merging occurring in future. This process includes two "Day 2 reports", which have been deployed daily since July 2020.*[54]

However, the ten breaches occurred between February and May 2020. This represents a failure on BOI's part to implement appropriate organisational security measures to identify the security issues or to take more timely mitigation to remediate the identified issues. When the coding error was discovered, BOI ought to have had measures in place to ensure the error was rectified quickly. A twenty one month delay is an unacceptably long rectification time, in particular for a coding error of this gravity. Therefore, I consider that the technical security measures in place at the time of the breach did not meet the standard required by the GDPR.

76. BOI also failed to perform sufficient testing on merged accounts. BOI points out that it has

> *oversight controls in place with its centralised account opening team whereby all account openings (i.e. 100% of all accounts opened by customers with BOI) are reviewed by management.*[55]

However, this applies to account openings, not account merging. Meanwhile, BOI's QA Procedures (10% sampling of merge) states that only 10% of merges are checked by random sampling.[56] I find this is an insufficiently low volume of testing considering the grave security

[54] Appendix C.9.1 BOI Submission 21 Dec 2022, page 8
[55] Appendix C.9.1 BOI Submission 21 Dec 2022, page 8
[56] Appendix C.4.5

risks that can result from such merging such as an unauthorised person accessing an account. I find BOI infringed Article 5(1)(f) and Article 32(1) GDPR by failing to implement this testing.

(i) Organisational Measures

77. BOI was aware of the issue of concern with the CIS as it was originally identified in 2019 by a Group Internal Audit. However, nine out of the ten data breaches were notified to BOI by either a data subject or a third party, rather than through follow up action to eliminate the impact identified in the BOI audit. This indicates that BOI was not carrying out appropriate testing or organisational measures as the breaches were reported by a data subject or a third party, as opposed to being identified by internal testing.

78. BOI states that

> *In October 2022, with a view to improving the effectiveness of measures in place and oversight, the teams for errors management assurance, data management and data remediation for the retail division were consolidated under single management within retail risk management partners.*[57]

While the DPC welcomes this measure, it was not in place prior to, or at the time of the breaches, which are the subject of this inquiry.

79. The sequence of breaches indicates a failure to act to adjust the effectiveness of ongoing technical and organisational measures on becoming aware of earlier breaches in order to adequately mitigate the risks. The Article 32(1)(d) GDPR requirement for regularly testing, assessing and evaluating the effectiveness of the measures must be matched to a requirement pursuant to Article 32(1)(b) to take new measures when the existing measures are shown to be ineffective. Therefore, the oversight measures demonstrated by BOI did not meet the standard required by the GDPR. I therefore find BOI infringed Article 5(1)(f) and Article 32(1) GDPR by failing to have adequate oversight measures in place.

H. Findings

80. For the reasons set out above, I find that BOI

- 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 and
- 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 BOI Banking 365 platform.

[57] Appendix C.9.1 BOI Submission 21 Dec 2022, page 6

I. Decision on Corrective Powers

81. I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that BOI has infringed Articles 5(1)(f) and 32(1) GDPR.

82. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. 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.

83. 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...*

84. Having carefully considered the infringements identified in this Decision, I have 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 I have decided are appropriate to address the infringements in the particular circumstances are:

    a. An order pursuant to Article 58(2)(d) GDPR to BOI to bring its processing operations into compliance with the GDPR in the manner specified below;

    b. A reprimand to BOI pursuant to Article 58(2)(b) GDPR; and

    c. One administrative fine of €750,000 for infringement of Article 5(1)(f) GDPR.[58]

85. I set out further detail below in respect of each of these corrective powers and the reasons why I have decided to exercise them.

J. Order to Bring Processing into Compliance

86. 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*

87. In circumstances where I have found that the processing at issue was not in compliance with the GDPR, I make an order pursuant to Article 58(2)(d) GDPR. Therefore, I order BOI to bring

[58] BOI Group worldwide annual turnover 2021 was €2,855M (See Bank of Ireland Group plc Annual Report 2021). Net Interest Income €2,219M + Total Business Income €636M = Total: €2,855M. 2% of this figure amounts to €57.1M. 4% of this figure amounts to €114.2M.

the relevant processing into compliance with Articles 5(1)(f) and 32(1) GDPR in the terms set out in the table below through implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks.

88. It is my view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with Articles 5(1)(f) and 32(1) GDPR. In this regard, I acknowledge BOI's on-going remedial actions, as outlined in submissions throughout the Inquiry.

89. The orders I am imposing are set out in the following table:

Number	Infringement and Action	Timescale
1.	Articles 5(1)(f) and 32(1) GDPR Lack of robust validation procedures and quality assurance controls. I order BOI to upgrade its validation controls in relation to data input by staff, as well as data in the CIS, in order to ensure the integrity, confidentiality and security of that data relating to BOI's obligations under Article 5(1)(f). I order BOI to implement quality assurance controls to ensure this upgraded procedure is followed relating to BOI's obligations under Article 32(1).	BOI is required to confirm to the DPC within 90 days of receiving this Decision that this order has been complied with.
2.	Articles 5(1)(f) and 32(1) GDPR Lack of emphasis in training materials on the importance of regular data protection and awareness training to staff, as well as training related to merging client data and how to prevent manual errors relating to BOI's obligations under Article 5(1)(f).. I order BOI to implement relevant training for staff relating to BOI's obligations under Article 32(1) GDPR.	BOI is required to confirm to the DPC within 90 days of receiving this Decision that this order has been complied with.
3.	Articles 5(1)(f) and 32(1) GDPR Lack of robust testing measures I order BOI to implement appropriate testing measures so as to reduce the risk of further coding errors occurring with the Banking 365 Service relating to BOI's obligations under Articles 5(1)(f) and 32(1) GDPR.	BOI is required to confirm to the DPC within 90 days of receiving this Decision that this order has been complied with.
4.	Articles 5(1)(f) and 32(1) GDPR Lack of emphasis on remediating errors quickly I order BOI to implement a process which ensures that any coding errors discovered in relation to the Banking 365 Service which allow unauthorised access to customer accounts are remediated without delay	BOI is required to confirm to the DPC within 90 days of receiving this Decision that this order has been complied with.

	relating to BOI's obligations under Articles 5(1)(f) and 32(1) GDPR.	

90. My decision to impose the orders is made to ensure that full effect is given to BOI's obligations under Articles 5(1)(f) and 32(1) GDPR. I consider that these orders are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

91. I consider that these orders are necessary to ensure that full effect is given to BOI's obligations in relation to the data security infringements outlined above, having particular regard to the high quantity, highly sensitive personal data of data subjects processed by BOI via Banking365.

92. The substance of these orders is the only way in which the defects pointed out in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that I am of the view that this power should be imposed.

93. Having regard to the non-compliance identified in this Decision, in my view, such orders are proportionate and are the minimum orders required in order to guarantee that compliance will take place in the future. I am satisfied that the orders are a necessary and proportionate action.

94. I therefore require BOI to comply with the above orders within the time specified from the date of notification of this decision. Further to this, I require BOI to submit a report to the DPC within a further month detailing the actions it has taken to comply with the orders.

K. Reprimand

95. 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*

96. I issue BOI with a reprimand in respect of its infringements of Article 5(1)(f) and Article 32(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The infringements contributed to a higher risk of fraud and financial loss in respect of the data subjects. Reprimands are appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance. The reprimand is necessary and proportionate in addition to the order in Part I of this Decision. While the order would require specific remedial action on the part of BOI, the reprimand formally recognises the serious nature of these infringements. I consider that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by BOI and other controllers or processors carrying out similar processing operations. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that BOI and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations with regard to the security of personal data.

L. Administrative Fines

97. 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*

98. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the order and reprimand also imposed in this Decision. Section 115 of the 2018 Act mirrors this by providing that the DPC may do either or both of imposing an administrative fine and exercising any other corrective power specified in Article 58(2) GDPR.

99. Article 83(1) GDPR provides:

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

100. Article 83(2) GDPR provides that when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to the following:

> *(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*

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

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

101. The decision as to whether to impose an administrative fine in respect of an infringement is a cumulative decision which is taken having had regard to all of the factors as set out in Article 83(2)(a) to (k) GDPR. Therefore, I will now proceed to consider each of these factors in turn in respect of each of the individual infringements identified in this Decision respectively.

102. In applying the Article 83(2)(a) to (k) GDPR factors to the infringements, I have set out below my analysis of the infringements collectively, where it is possible to do so. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, I have considered the infringement of Article 5(1)(f) GDPR and the infringement of Article 32(1) GDPR separately when deciding whether to impose an administrative fine in respect of each infringement. I have made a separate decision on each infringement, and I have made each decision without prejudice to any factors arising in respect of the other infringement. For the avoidance of doubt, my decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement. In its submission, BOI wished it stated that *"BOI has reserved its position in relation to Article 83(3) GDPR."*[59]

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;

103. In considering the nature, gravity and duration of BOI's infringements, I have had regard to the analysis in Part F of this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) GDPR requires that I have due regard to the nature, gravity and duration of the infringement. Article 83(2)(a) GDPR also requires me to have due regard to the number of data subjects affected by the infringement and the level of damage suffered by them.

104. Therefore, I will first consider these issues before proceeding to consider the nature, gravity and duration of the infringements.

105. The key risk arising from this processing was that an unauthorised person could gain access to a customer's account and/or be able to use any or all of the elements of the service listed

[59] Appendix C.9.1 BOI Submission 21 Dec 2022, page 15

above. This would result in a high risk of fraud and/or identity theft which would severely undermine a customer's relationship with the bank and pose a particularly high risk to vulnerable users. In addition, because the Banking365 app was offered as an access method for the majority of the customer base, the likelihood of any error resulting in a personal data breach was higher. Ten data subjects were affected by the personal data breaches considered in this Decision through having their personal data erroneously disclosed to unauthorised people.

106. BOI's infringement of Articles 5(1)(f) and 32(1) GDPR includes the failure to ensure appropriate security of the data and failure to implement technical and organisational measures appropriate to the level of risk incurred to data subjects as a result of BOI's processing of personal data on Banking365. BOI failed to implement measures that ought to have been in place in order to protect the rights and freedoms of each data subject from the start of the temporal scope. The failure to implement the necessary safeguards in an effective manner at the appropriate time led to customers' personal data being erroneously disclosed to unauthorised people.

107. In assessing the level of damage suffered by the data subjects, I have had regard to the loss of control suffered by them over their personal data. The personal data affected by the breaches included sensitive financial and economic personal data, which are private matters kept strictly confidential by most people.

108. In assessing the level of damage for the purpose of Article 83(2)(a) GDPR, it is therefore appropriate that I have regard to the likely level of damage suffered by data subjects (including non-material damage).

The nature of the infringements

109. The nature of BOI's infringements of Articles 5(1)(f) and 32(1) GDPR concern its failure to implement appropriate measures designed to implement data-protection principles in an effective manner; and to integrate appropriate technical and organisational measures, including training, to ensure that personal data are not made accessible, without the individual's intervention, to unauthorised natural persons. Having regard to the nature and scope of the data processing, I consider that this failure to implement appropriate measures by BOI to be serious.

The gravity of the infringements

110. In assessing the gravity of the infringements, I have had regard to the number of data subjects affected and the level of damage suffered by them. The breaches affected 10 data subjects, that BOI is aware of; however, potentially a much wider range of BOI customers were at risk. I note that BOI pointed out that *"[n]one of the 136 customers affected by over-merging suffered any financial loss as a result of the error."*[60] I have also had regard to how the infringements increased the risks posed by the processing to the rights and freedoms of BOI Banking365 users. These risks include the risk of unauthorised access and unauthorised

[60] Appendix C.9.1 BOI Submission 21 Dec 2022, page 13

disclosure of personal data to third parties of personal data processed within the platform, as well as the risk of fraud and financial loss.

111. In those circumstances, I find that the gravity of BOI's failure to *implement appropriate technical and organisational measures* that were sufficient *to ensure a level of security appropriate to the risk* is serious.

The duration of the infringements

112. The duration of BOI's infringements of Articles 5(1)(f) and 32(1) GDPR regarding the processing commenced at the application of the GDPR on 25 May 2018. The obligation to implement the appropriate organisational and technical measures required by these Articles applied from 25 May 2018. The infringement was ongoing from the application of the GDPR until the commencement of this inquiry (the temporal scope). 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 under Articles 5(1)(f) and 32(1) GDPR lasted at least from 25 May 2018 until the Commencement of this inquiry on 12 August 2020.

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

113. In assessing the character of the infringement, I note that the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either *'intentional'* or *'negligent'*. The WP29 considered this in its *'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679'* (the **'Administrative Fines Guidelines'**) as follows:

> *In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*[61]

114. The Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence was present in a particular case:

> *The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.*[62]

115. In determining whether an infringement was intentional, I must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration.

116. In determining whether an infringement was negligent, I must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

---

[61] C.9.2, page 11.

[62] C.9.2, page 12.

For the avoidance of doubt, the DPC is solely considering whether the infringements are negligent by reference and within the meaning of Article 83(2)(b) GDPR.

117. As compliance with the GDPR Articles is measured in terms of compliance with clear obligations on controllers and processors, to find any infringement there must have been either an intentional or a negligent failure to meet those obligations. If the infringement has an intentional character then it indicates a more serious infringement and if it has a negligent character then it has a lower severity.

118. BOI's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing, concerns its failure to implement appropriate measures to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing. Hence, the characteristics of this infringement concerns that lack of appropriate technical and organisational measures for the duration of the infringement. In order to classify these infringements as intentional, I must be satisfied that (i) BOI 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.

119. Having considered the objective elements of BOI's conduct, as set out above, there is evidence that BOI knew that its measures were not sufficient in respect of the need to implement the data protection principles in an effective manner. Despite knowledge of ongoing data breaches, it is apparent that the measures implemented were ineffective until the end of the temporal scope, including a 21 month delay in successfully implementing the technical fix required for the CIS. I note BOI's statement that this delay was partly as a result of *"the impact of COVID-19 in this time period and the caution required for technical changes to our core system."*[63] I do not consider that BOI wilfully omitted to implement appropriate measures. While BOI's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 32(1) GDPR), I do not consider that this failure was wilful on BOI's part. However, it is clear that BOI ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 32(1) GDPR. I find that BOI's failure to implement appropriate measures pursuant to Articles 5(1)(f) and 32(1) GDPR in respect of its processing was negligent in the circumstances.

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

120. Section E of this Decision outlines the mitigating measures that BOI put in place after it discovered the data breaches. I note that according to BOI

> *a comprehensive investigation was carried out by the Bank into over-merging with all potential and possible cases being identified and reviewed on a case by case basis.*[64]

Once appropriate measures were fully implemented, the particular breaches were prevented. However, it took over two years from discovery of the issues with the CIS for the

[63] Appendix C.9.1 BOI Submission 21 Dec 2022, page 7

[64] Appendix C.9.1 BOI Submission 21 Dec 2022, page 13

errors caused by these issues to be be fully remediated, bearing in mind the impact of Covid-19 and the complexity of the issue as pointed out by BOI in their December 2022 submission. I also note that *"no instances of fraud or identity theft have been identified to date"*[65] by BOI. Howover, it is not always possible to retrospectively apply mitigation that will effectively correct a past lack of control, as personal data has already been breached and data subjects may already have suffered consequential damage as a result.

121. I note that the above actions by BOI may have reduced the probability of further breaches causing additional risk of damage to data subjects after the infringements occurred for the purpose of Article 83(2)(c) GDPR. Having regard to these actions for the purpose of Article 83(2)(c) GDPR, I am of the view that the actions provided limited mitigation of the damage to data subjects, and accordingly I consider that the actions are of mitigating value.

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 GDPR;

122. The Administrative Fines Guidelines set out that:

> *The question that the supervisory authority must then answer is to what extent the controller "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.*[66]

123. Article 25 is not within the scope of this inquiry.

124. I have found that BOI infringed Article 32(1) GDPR (as well as Article 5(1)(f) GDPR) regarding its processing of personal data via the Banking365 app. I consider that BOI holds a high degree of responsibility for this infringement and that the absence of sufficiently robust technical and organisational measures must be deterred. It is clear that BOI did not do *"what it could be expected to do"* in the circumstances assessed in this Decision.

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

125. BOI was fined, reprimanded and ordered to bring its processing into compliance in March 2022 for infringments of Article 32(1) GDPR, as well as Articles 33 and 34 GDPR.

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;

126. BOI submitted breach notification forms in respect of the personal data breaches to the DPC and gave updates regarding BOI's progress in remediating the breaches. I acknowledge BOI's cooperation with the DPC during the course of the Inquiry and I also note that this co-operation was of *"a timely, collaborative and forthcoming"* nature.[67] However, I note that BOI

---

[65] Appendix C.9.1 BOI Submission 21 Dec 2022, page 13

[66] Article 29 Data Protection Working Party 'WP253:Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' (endorsed by EDPB) at page 13. Note that new EDPB Guidelines 04/2022 have been published which cite the previous WP253 Guidelines. After public consultation, submissions on the revised Guidelines are currently (November 2022) under consideration by the EDPB.

[67] Appendix C.9.1 BOI Submission 21 Dec 2022, page 14

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.

127. I wish to note that the measures implemented by BOI as part of their Group Internal Audit which first identified the issue with the CIS in 2019 and the steps taken by BOI to remediate the infringement. However, I note that it is not possible to fully remediate the adverse effects on BOI365 users (in terms of the previous lack of control over personal data leading to unauthorised disclosure).

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

128. The personal data affected by the infringement included sensitive financial and economic personal data. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to financial fraud and/or identity theft.

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;

129. BOI reported the existence of the personal data breaches to the DPC without undue delay. However, BOI's compliance with its own obligation to notify personal data breaches under Article 33(1) GDPR cannot be considered mitigating in respect of the infringements of Articles 5(1)(f), and 32(1) GDPR.

130. BOI also co-operated with the DPC in sending particulars of the technical and organisational measures in place at the time of the personal data breach when requested to do so by the DPC.

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

131. Corrective powers have not previously been ordered against BOI with regard to the subject matter of this Decision.

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

132. Such considerations do not arise in this case.

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.

133. I am of the view that there are no other aggravating or mitigating factors in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR.

M. Decisions on Whether to Impose Administrative Fines

134. In deciding whether to impose an administrative fine in respect of the infringement of Articles 5(1)(f) and 32(1) GDPR, I have had regard to the factors outlined in Article 83(2)(a) – (k) GDPR cumulatively, as set out above. I have also had regard to the effect of the order and reprimand imposed in ensuring compliance with the GDPR. The order will assist in ensuring compliance by mandating specific action on the part of BOI in order to re-establish compliance. The reprimand will contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements. However, I consider that these measures alone are not sufficient in the circumstances to ensure compliance. I find that an administrative fine in respect of the infringement of Article 5(1)(f) GDPR is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

135. 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 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.*

136. While the order to bring processing into compliance imposed in this Decision will re-establish compliance with the GDPR with respect to the infringements identified, I do not consider this measure appropriate to deter other future serious infringements. While the reprimand will assist in dissuading BOI and other entities from similar future non-compliance, in light of the seriousness of the infringements, I do not consider that the reprimand alone is proportionate or effective to achieve this end. I find that an administrative fine is necessary in respect of the infringement of Article 5(1)(f) to deter other future serious non-compliance on the part of BOI and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

(1) The infringement of Articles 5(1)(f) is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Data subjects' financial information was accessed by unauthorised people and the data subjects were exposed to the risks of fraud, I

consider that BOI's non-compliance with its security obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects. Therefore, I consider that an administrative fine is appropriate and necessary in order to dissuade non-compliance.

(2) Having regard to the nature, gravity and duration of the infringements, I also consider that administrative fines are proportionate in the circumstances in view of ensuring compliance. The loss of control suffered by the data subjects as a result of BOI's infringement of Article 5(1)(f) caused data breaches which affected 10 data subjects. I consider that the unauthorised access to financial data constitutes significant damage in the circumstances. In light of this damage, I consider that a fine is proportionate to responding to BOI's infringement of Article 5(1)(f) with a view to ensuring future compliance. I consider that fine does not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

(3) I consider that the negligent character (within the meaning of Article 83(2)(b) GDPR) of BOI's infringement of Articles 5(1)(f) GDPR carries weight when considering whether to impose an administrative fine, and if so, the amount of the fine. For example, there was an approximately two year gap between BOI identifying the overmerging issue on the CIS, via its internal audit, and providing a final technical fix.

(4) I consider that the administrative fine would help to ensure that BOI 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. In these particular circumstances where the categories of users' data affected by BOI's infringements carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud, I consider that an administrative fine is appropriate.

(5) I have given regard to the relatively low number of notified breaches in relation to the number of BOI's customers. I have also had regard to the actions taken by BOI in order to minimise further breaches (as assessed above pursuant to Articles 83(2)(c) and (f) GDPR). I consider that these factors mitigated the damage to data subjects to an extent, and remedied the infringements to an extent. I have therefore taken these mitigating actions into account when calculating the administrative fine. However, despite these factors, I consider that an administrative fine is appropriate, necessary and proportionate in respect of these infringements in order to ensure compliance with the GDPR. While the lack of previous relevant infringements is a mitigating factor, I consider that the need to dissuade non-compliance of this nature far outweighs the mitigation applied for this factor. Furthermore, despite the actions taken to mitigate against further breaches, the damage suffered as a result of the infringements has not been significantly mitigated for the affected data subjects. In light of the negligent character of the infringements, and BOI's failure to comply with its obligations with regard to data protection, I consider that a dissuasive administrative fine is necessary in the circumstances to ensure future compliance

137. Based on the analysis I have set out above, I impose the following administrative fine:

1) In respect of BOI's infringement of Article 5(1)(f) GDPR regarding the processing, I impose a fine of €750,000.

138. In the Draft Decision, I proposed a fining range of between €500,000 and €900,000 for BOI's infringement of Article 5(1)(f). Having considered BOI's submissions I consider that €750,000 is an appropriate figure.

139. In having determined the quantum of the fine above, I have taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *effective, proportionate and dissuasive* in each individual case. My view is that, in order for any fine to be *effective*, it must reflect the circumstances of the individual case. As outlined above, the infringements are all serious in nature and in gravity. The infringements concern the personal financial data of Banking365 users and the infringements increased the risks posed by the processing to the rights and freedoms of those data subjects, in particular in relation to the risk of financial fraud.

140. In order for a fine to be *dissuasive*, it must dissuade both the controller/processor concerned, as well as other controllers and processors carrying out similar processing operations, from repeating the conduct concerned.

141. As regards the requirement for any fine to be *proportionate*, this requires me to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fine imposed above does not exceed what is necessary to enforce compliance with the GDPR.

142. I am satisfied that the range for the fine specified above, if imposed on BOI, would be effective, proportionate and dissuasive, taking into account all of the circumstances covered by the Inquiry.

Article 83(3) GDPR

143. Article 83(3) GDPR provides that:

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

144. I am imposing an administrative fine for BOI's infringement of Article 5(1)(f). This infringement itself is the gravest infringement and I am acting in accordance with Article 83(3) in imposing this fine.

Article 83(5) GDPR

145. As regards the maximum amount for the fine that can be imposed in respect of the infringement of Article 5(1)(f) GDPR, the relevant fining cap is the higher of €20,000,000 or 4% of the worldwide annual turnover of the preceding financial year. Therefore, I find that

the cap for an infringement of Article 5(1)(f) GDPR is €114.2 million.[68] This figure is not a starting point, but rather the cap on the permitted range as provided for in Article 83(5) GDPR. The fine imposed is below 4% of the turnover of BOI.

146. It is my view that the above administrative fine meets the requirements of being effective, proportionate and dissuasive as required by Article 83(1) GDPR. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fine imposed does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringement on the data subject rights enshrined in the GDPR. Accordingly, I am satisfied that the fine I have decided to impose is effective, proportionate and dissuasive, taking into account all of the circumstances of the inquiry.

N. Right of Appeal

147. This Decision issues in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, BOI has the right to appeal against this Decision within 28 days from the date on which notice of this Decision is received by it. Furthermore, pursuant to section 142 of the 2018 Act, as this Decision includes a decision to impose an administrative fine, BOI will also have the right to appeal against that Decision within 28 days from the date on which notice of the Decision is given to it.

[68] BOI Group worldwide annual turnover 2021 was €2,855M (See Bank of Ireland Group plc Annual Report 2021). Net Interest Income €2,219M + Total Business Income €636M = Total: €2,855M. 2% of this figure amounts to €57.1M. 4% of this figure amounts to €114.2M.