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

DPC Case Reference: IN-19-9-5

In the matter of Bank of Ireland

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

14 March 2022

Contents

1. Introduction

1.1 This document is a decision (the **"Decision"** or the **"Final Decision"**) made by the Data Protection Commission (the **"DPC"**) in accordance with section 111 of the Data Protection Act 2018 (the **"2018 Act"**). I make this Decision having considered the information obtained in the separate own volition Inquiry (the **"Inquiry"**) conducted by authorised officers of the DPC pursuant to section 110 of the 2018 Act (the "**Case Officers**"). The Case Officers provided Bank of Ireland Group plc (**"BOI",** the **"data controller"** or the "**controller**"**)** with the Draft Inquiry Report and the Final Inquiry Report.

1.2 BOI was provided with the draft decision in this Inquiry on 12 January 2022 (the "**Draft Decision**") to provide it with a final opportunity to make submissions. 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.

1.3 This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (Regulation (EU) 2016/679) (the **"GDPR"**) arising from the infringements that have been identified herein. In this regard, BOI is required to comply with these corrective powers and it is open to this office to serve an enforcement notice on BOI in accordance with section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

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

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

ii. Legal Basis for the Decision

2.1 The decision-making process for this Inquiry is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to

decide on the corrective powers, if any, to be exercised. As the sole member of the DPC, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Case Officer as well as any other materials that BOI has furnished to me, and any other materials that I consider relevant, in the course of the decision-making process.

2.2 The Final Inquiry Report was transmitted to me on 19 March 2021, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and BOI; and copies of all submissions made by BOI, including the submissions made by BOI in respect of the Draft Inquiry Report. A full schedule of all documentation considered by me for the purpose of this Decision is appended hereto. I issued a letter to BOI on 10 November 2021 to notify it of the commencement of the decision-making process, and circulated the Draft Decision to BOI on 12 January 2022. BOI made submissions on the Draft Decision on 2 February 2022.

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

3. Findings of Fact

3.1 During the period 9 November 2018 to 27 June 2019, the DPC received 22 breach notifications from BOI in relation to corruption of information in the BOI's data feed to the Central Credit Register (**"CCR"**).

3.2 The CCR is a centralised system that collects and securely stores information about loans. The CCR is managed by the Central Bank of Ireland, (**"the CBI"**) under the Credit Reporting Act 2013 (**"the 2013 Act"**). "Credit Information Providers," as defined under section 2(1) of the 2013 Act have obligations to upload information to the CCR specified in section 11 of the 2013 Act and in the secondary legislation made pursuant to it.[1] Section 11(5) makes provision for lenders submitting information on loans of €500 or more to the CCR. This information is used to generate individual credit reports on borrowers, which they and, in certain circumstances, lenders can access. Borrowers can request their credit report to see what information lenders have submitted on their loans. Lenders can use credit reports to get a picture of a borrower's current lending and credit history. This helps a lender to decide if it should approve an application for a loan or not. The Central Bank also uses the CCR to get better insights into the level and patterns of lending in the economy.

3.3 It is noted that seven of the notified incidents also involve the transfer of data including personal data to the Irish Credit Bureau (the **"ICB"**). The ICB has recently been wound

[1] S.I. No. 486/2016 - Credit Reporting Act 2013 (Section 11) (Provision of Information for Central Credit Register) Regulations 2016.

up and those Credit Information Providers as defined under section 2(1) of the 2013 Act will now rely upon their own internal information in order to approve an application for a loan, coupled with the information contained within the CCR database.

3.4 Following an examination of the notifications, the DPC was of the opinion that one or more provisions of the 2018 Act or the GDPR may have been contravened in relation to the processing of personal data relating to data subjects in respect of which BOI is the data controller for the purposes of the Act and the GDPR.

3.5 In reviewing the matters raised in the breach notifications, the DPC considered it appropriate to establish a full set of facts so that it could assess whether or not BOI has discharged its obligations as data controller in connection with the subject matter of the breaches and determine whether or not any provision(s) of the 2018 Act or the GDPR had been contravened by BOI in that context.

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

4. Scope of the Inquiry

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine whether or not BOI discharged its obligations in connection with the subject matter of the personal data breaches notified by it 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.

5. Issues for Determination

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

- Preliminary Issue: Whether the incidents described in the breach notifications reported by BOI to the DPC fall within the definition of a "*personal data breach*" under Article 4(12) of the GDPR;
- Issue 1: Whether BOI has infringed Article 33 of the GDPR in the manner in which it reported personal data breaches (if any personal data breaches are found in this Decision) to the DPC;
- Issue 2: Whether BOI has infringed Article 34 of the GDPR; and
- Issue 3: Whether BOI has infringed Article 32 of the GDPR.

6. Preliminary Issue: Article 4(12) of the GDPR

6.1 The majority of breach notifications made by BOI to DPC concerned inaccurate customer data uploaded to the CCR by BOI which gave an erroneous view of BOI's customers' finances and credit history. A key preliminary issue that arises is whether the incidents described in the 22 breach notifications made by BOI to the DPC fall within the definition of a "*personal data breach*" under Article 4(12) of the GDPR.

6.2 Article 4(12) of the GDPR defines a "*personal data breach*" as meaning "*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*."

6.3 The Article 29 Working Party, in its *Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)* (as adopted by the EDPB) (the "**Breach Notification Guidelines**") opined that breaches can be categorised according to three well-known security principles: [2] a *"confidentiality breach,"* where there is an unauthorised disclosure of, or access to, personal data; an *"integrity breach,"* where there is an unlawful or accidental alteration of personal data; and an *"availability breach,"* where there is an accidental or unlawful loss of access to, or destruction of, personal data.[3]

6.4 On the facts of this Decision, out of the three types of personal data breaches described, the majority of breach notifications in this case most closely resemble an "*integrity breach*" in that customer data was inaccurately altered. However, many of the breach notifications made to the DPC by BOI have characteristics of a "*confidentiality breach*". Some breach notifications revealed that BOI disclosed personal data to the CCR which was not required under the terms of the 2013 Act. Insofar as BOI uploaded inaccurate customer data to the CCR, this could also be described as a "*confidentiality breach*" in that BOI only had the statutory authority to upload accurate customer data to the CCR.

6.5 Many breach notifications also have characteristics of an *"availability breach"*. This is evident from the Breach Notification Guidelines:

"The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12)."

6.6 Where due to a default in a system, personal data is made inaccurate this can be classified as an "*availability breach*" as the original personal data is temporarily lost.

[2] At p7

[3] Ibid, combined with wording from Article 4(12) of the GDPR

6.7 Some of the incidents that arose in this Inquiry involved an alteration of personal data on BOI's systems that, when uploaded to the CCR or the ICB, undoubtedly resulted in a risk to data subjects. A question mark was raised in the Inquiry Report about the extent to which these incidents arose as a result of a "*breach of security*" within the meaning of Article 4(12) of the GDPR[4] due to the fact that there was no unauthorised disclosure of personal data in those cases. I agree with the Inquiry Report and with BOI's submissions that a "*breach of security*" must *lead to* the impact to personal data in question.[5] However, it is clear from the list of impacts to personal data in Article 4(12) that personal data breaches are not limited to "*unauthorised disclosure*" and can include "*accidental or unlawful*" alteration of personal data. More generally, the concept of "*breach of security*" is most clearly defined by reference to the measures that can be put in place to prevent the specific risks to personal data listed in Article 4(12). Under Recital 49 of the GDPR, "*network and information security*" is explained to be "*the ability of a network and information system to withstand, at a given level of confidence*" the types of incidents listed in Article 4(12) of the GDPR (i.e. the ability to withstand accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data). Those aims of technical and organisational security are also set out in Article 32(1) of the GDPR. In particular Article 32(1)(b)-(c) indicate that security measures include:

> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; [and]*
> *(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.*

Based on the wording of the GDPR more generally, including Article 32(1), it is clear that '*security'* can be understood to comprise both technical and organisational measures.

6.8 Based on these aspects of the GDPR, the definition of a personal data breach can be considered to have three elements. There must be (*1*) an incident (*2*) that has one of the impacts to personal data listed in Article 4(12) (*3*) that a network and information system was unable to withstand, at a given level of confidence. The inability of a system to withstand the incident or the impact to personal data is a "breach of security" which, although fundamentally interlinked with the impact to personal data arising from the breach, relates to the inability of a system to withstand the impact, and is therefore distinct from the impact to personal data itself. It is also worth noting that for a personal data breach to occur it is not necessary that a third party has been involved in the occurrence of the incident. A breach of security pertaining to any personal data *'transmitted, stored or otherwise processed*' falls within the scope of Article 4(12) of the GDPR. The Breach Notification Guidelines make this clear by stating (emphasis added):

[4] At p45 of the Final Inquiry Report it states: "The notifications were submitted to the DPC under Article 33(1) of the GDPR, however in these cases the circumstances may not strictly meet the definition of a '*personal data breach*' under Article 4(12) of the GDPR" in paragraph 206

[5] BOI Submissions 2 February 2022, [3.2]

It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, ***but includes incidents from internal processing that breach security principles***.[6]

6.9 In the context of altered data, a "*breach of security*" is thus not limited to a technical incident or an unauthorised disclosure of personal data, and can include internal processing operations that result the accidental or unlawful alteration of personal data. Thus, an incident that results in the accidental or unlawful alteration of personal data that a system was unable to withstand through technical or organisational measures falls within the definition of a "*personal data breach*."

6.10 A few other points about this interpretation are worth highlighting. The existence of a personal data breach is not conclusive in itself that there has been an infringement of any provisions of the GDPR. Articles 33(1) and 34(1) trigger notification obligations on the basis of risks arising from personal data breaches. Articles 5(1)(f) and 32(1) place an obligation on controllers to put in place technical and organisational security measures *appropriate* to the risk arising from the processing in question. Article 5(1)(d) sets out the accuracy principle which states that personal data shall be "*accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*."

6.11 In relation to the interaction between these provisions of the GDPR and the definition of a '*personal data breach*,' BOI's submissions argue that the "*requirements in Articles 33 and 34 are important in the context of safeguarding the rights of data subjects (see further below), they are not in our view intended to apply to every breach of the accuracy principle under Article 5(1)(d)… Given that paragraph 9.2 of the Draft Decision acknowledges that 'Article 32 should be interpreted in light of other Articles of the GDPR such as Article 5', we would submit that Article 4(12) should similarly be interpreted in light of Article 5(1)(d)*."[7] It is accepted that it is conceivable that circumstances may arise where the accuracy principle could be infringed without there being a "*personal data breach*" within the meaning of Article 4(12) of the GDPR. However, I am not convinced by the submission that Article 4(12) can be interpreted in light of Article 5(1)(d) in the manner set out. Articles 5(1)(d), 5(1)(f) and 32(1) relate to the appropriateness or reasonability of technical and organisational measures actually applied. Interpreting the definition of '*personal data breach*' by reference to an assessment of whether appropriate or reasonable measures had been put in place could lead to anomalous results. For example, it could result in a controller deciding not to report a major loss of personal data due to a sophisticated and unprecedented cyberattack because it had put in place what it reasonably considered to be appropriate security measures on the basis of the state of the art. Instead, as outlined above, a "*breach of security*" can be considered to be the inability of a network and information system to withstand certain harms to personal data. That inability is not in itself conclusive either way that any additional security measures would be appropriate or

[6] Breach Notification Guidelines, p7 at footnote 13

[7] BOI Submissions 2 February 2022, [3.4]

reasonable. However, that inability does form a constituent part of the determination that a "*personal data breach*" has occurred.

6.12 The submissions draw attention to certain sections of the CRA 2013 and associated secondary legislation. As highlighted in the submissions, section 21 of the CRA 2013 states (BOI's emphasis),

> *A credit information provider shall take reasonable steps to verify that the information which the credit information provider obtains from credit information subjects is accurate and complete.*

6.13 The submissions also highlight Regulation 6 of the Credit Report Act 2013 (Section 11) (Provision of Information for Central Credit Register) Regulations 2016 states (BOI's emphasis),

> *A credit information provider shall—*
>
> *(a) take all reasonable steps to ensure the accuracy of the personal information provided to the Bank pursuant to Regulation 3, and*
>
> *(b) inform the Bank of any changes to the personal information provided to the Bank pursuant to Regulation 3 of which it becomes aware.*

6.14 The submissions argue that '*in determining what constitutes a "breach of security" in the context of the CCR… in our view regard should be had to whether BOI (or any CIP) has met, or failed to meet, the reasonableness requirements outlined above*.'[8] The submissions also highlight that certain sections of the CRA 2013 were amended when the 2018 Act was brought in but the above provisions were not.[9]

6.15 I take note of the reasonability threshold in these statutory provisions and the overlap with the wording of the accuracy principle in Article 5(1)(d). I also note the fact that, as highlighted by BOI, these provisions were not amended to take account of the GDPR despite the opportunity to do so. However, as noted above, I do not consider it appropriate to determine whether a personal data breach has occurred by reference to the reasonability of measures applied. Moreover, in line with principles of statutory interpretation, to the extent that the CRA 2013 suggests an approach less protective of personal data than the GDPR or the 2018 Act, the approach set out in the GDPR and 2018 Act must prevail.[10] While the CRA 2013 regime is specific to the CCR environment, the GDPR and the 2018 Act are specific to the protection of personal data. Therefore, while it is arguable whether the uploading of inaccurate information to the

[8] Submissions of 2 February 2022, 4.4

[9] Ibid, 4.3

[10] See section 6 of the Interpretation Act 2005, which states, "In construing a provision of any Act or statutory instrument, a court may make allowances for any changes in the law, social conditions, technology, the meaning of words used in that Act or statutory instrument and other relevant matters, which have occurred since the date of the passing of that Act or the making of that statutory instrument, but only in so far as its text, purpose and context permit."

CCR amounts to a breach of the provisions of the CRA 2013, depending on the application of the reasonability test set out in that regime, it is a separate consideration whether the inaccuracy of any personal data on the CCR system constitutes a "*personal data breach*."

6.16 Following on from this analysis, in considering the following breach notifications, I have concluded that incidents reported by BOI fall within the scope of the definition of "*personal data breach*" under Article 4(12) of the GDPR where an event resulted in inaccurate data accidentally being reported to the CCR in circumstances where there was an inadequacy in BOI's technical and organisational measures. I note that the Final Inquiry Report identified a system inadequacy underpinning each of the incidents that I have identified as a personal data breach in the following section.[11] I have elaborated on this below, drawing on the submissions and documentation received from BOI throughout the Inquiry, and the factual findings in the Inquiry Report about the deficits in information security that contributed to each incident. I consider that performing this analysis in this way is appropriate in the circumstances of this Inquiry, where there has been a question mark cast over the definition of a "*personal data breach*" and its application to the facts at hand. In those circumstances, it is fair to BOI that I consider the application of the "*breach of security*" aspect of the definition of "*personal data breach*" in this way. This Decision should not form a precedent for controllers in other circumstances to take an overly technical interpretation of the definition of "*personal data breach*" when considering their obligations under the GDPR – the focus of controllers should first and foremost be on the risk to data subjects arising from an event and whether notifying an incident would assist with the protection of data subjects' rights. In this Inquiry too, based on the analysis in relation to Articles 33 and 34 of the GDPR in the sections below, it is clear that there was a risk to data subjects in the circumstances at hand, and BOI was correct to notify these incidents to the DPC on that basis.

6.17 I will now consider each breach notification in turn and explain why I consider it to be correctly classified as a "*personal data breach*" under Article 4(12) of the GDPR in line with this interpretation.

1. BN- 18-11-134

6.18 On 9 November 2018, BOI submitted a personal data breach notification relating to the unauthorised disclosure of personal data from BOI to the CCR which occurred on 12 October 2018. The breach notification related to information in relation to 51 data subjects being provided to the CCR in error. Due to a manual error BOI uploaded personal data of borrowers which should not have been uploaded. The categories of personal data included in the disclosure to the CCR were economic and financial.

[11] Final Inquiry Report, [66], [85], [100], [111], [127], [138], [152], [162], [182], [196], [217], [225], [232], [241], [251], [263], [270], [284],[297]

6.19 I find *BN-18-11-134* meets the definition of a personal data breach under Article 4(12) of the GDPR. Article 4(12) of the GDPR includes an "*unauthorised disclosure*" of personal data. BOI explained that the incident resulted from a "*process gap due to design failure during initial upload of accounts*."[12] Here BOI also lacked the authority to upload the personal data of 51 data subjects to the CCR and thus committed a personal data breach.

2. BN-19-1-25

6.20 On 4 January 2019, BOI submitted a personal data breach notification relating to an unauthorised disclosure of personal data from BOI to the CCR. This breach notification described how details for customers residing in the United Kingdom were included in a submission to the CCR in error as a result of selection criteria not being implemented. The incident resulted from an error in the application of selection criteria,[13] which was remedied by introducing reporting flags to exclude non-resident borrowers.[14]

6.21 I find *BN-19-1-25* meets the definition of a personal data breach under Article 4(12) of the GDPR. Section 2(2) of the 2013 Act only requires BOI to upload details relating to customers who are resident in the state at the time the credit application or credit agreement is made or to which the law of Ireland applies. BOI thus lacked the authority to upload the information to the CCR.

3. BN-19-1-31

6.22 The incident occurred where BOI reported customers who were previously removed from their mortgage accounts to the CCR in error. This breach was reported to the DPC on 4 January 2019. The incident occurred as a result of original co-borrowers to a debt being reported in error to the CCR when the account was in fact closed. The incident affected 197 data subjects.

6.23 I find *BN-19-1-31* meets the definition of a personal data breach under Article 4(12) of the GDPR. The incident resulted from a "lack of understanding of a system feature when CCR reporting solution developed [sic] that did not distinguish between current and existing borrowers" which was remedied by a technical fix.[15] Moreover, in reporting inaccurate data to the CCR in respect of data subjects, BOI could be said to have ***altered*** those data subjects' personal data. "*Alteration*" is one of the incidents of a "*breach of security*" under Article 4(12) of the GDPR. It was also an unauthorised disclosure of personal data, as the personal data of those data subjects should not have been disclosed to the CCR.

4. BN-19-1-267

6.24 On 24 January 2019, BOI made a breach notification to the DPC where it reported business credit card balances to the CCR in circumstances where only the data subjects'

[12] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 1
[13] Final Inquiry Report, [83] citing Appendix D.1. BOI Breach notifications with correspondence. BN-19-1-25 page 87
[14] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 2
[15] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 3

personal credit cards and not their business credit cards should have been reported to the CCR. The categories of subject error included data subject identity, contact details and economic and financial data relating to business credit cards. 236 data subjects were affected by this incident.

6.25 I find *BN-19-1-267* meets the definition of a personal data breach under Article 4(12) of the GDPR. The incident resulted from a system feature "*that did not accurately flag the primary cardholder for Sole Trader Credit Cards.*"[16] In any event, in Article 4(12) of the GDPR an incident of breach of security is if there has been an "*unauthorised disclosure*" of personal data. Here BOI lacked the authority to upload the business credit card balances of data subjects to the CCR.

5. BN-19-3-33

6.26 On 1 March 2019, BOI submitted a personal data breach notification describing how incomplete balance details of customers had been uploaded to the CCR. On 21 June 2019, BOI subsequently informed the DPC that no account balances relating to individuals were incorrectly recorded on the CCR. In other words, on completing the investigation into the data sent to the CCR, BOI determined the data was not inaccurate.

6.27 I find that *BN-19-3-33* does not meet the definition of a personal data breach under Article 4(12) of the GDPR.

6. BN-19-4-117

6.28 On 4 April 2019, BOI submitted a personal data breach notification which noted debts relating to a limited company and partnerships were incorrectly recorded against individuals on the CCR. BOI explained the event occurred due to data subjects being incorrectly recorded as 'Sole Traders' on the credit card system which resulted in an unauthorised and inaccurate report to the CCR.

6.29 I find *BN-19-4-117* meets the definition of a personal data breach under Article 4(12) of the GDPR. As a result of an error on BOI's credit card system, customers' personal data was altered which resulted in inaccurate data being uploaded to the CCR. This falls within the definition of a personal data breach under Article 4(12) of the GDPR.

7. BN-19-4-302

6.30 On 12 April 2019, BOI submitted a personal data breach notification to the DPC which noted that details relating to approximately 14 accounts were reported to the CCR in error with a balance of zero outstanding. These accounts were out of scope for the CCR as they related to loans that had been repaid prior to the effective date of CCR reporting. The Final Inquiry Report concluded that the unauthorised disclosure occurred as a result of the fact that "*the technical and organisational measures in place at the time of the incident to ensure against the unauthorised or unlawful processing of personal data were inadequate*."[17] Additional training was carried out as a remediation measure.[18]

[16] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 4
[17] Final Inquiry Report, [138]
[18] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 7

6.31 I find *BN-19-4-302* falls within the definition of a personal data breach under Article 4(12) of the GDPR. As a result of BOI erroneously uploading these accounts to the CCR due to inadequate technical and organisational measures, an unauthorised disclosure of personal data occurred. This is within the scope of Article 4(12) of the GDPR.

8. BN-19-4-410

6.32 On 18 April 2019, BOI submitted a personal data breach notification to the DPC describing how it had incorrectly reported data subjects to the CCR who had been declared bankrupt or had exited personal insolvency arrangements. These categories of data subjects fall outside the scope of reporting obligations to the CCR.

6.33 I find *BN-19-4-410* falls within the definition of a personal data breach under Article 4(12) of the GDPR. The incident resulted from "*inadequate controls over the processing of a tactical file used to manage the scope of reporting for bankrupt customers*."[19] As a result of BOI erroneously uploading these accounts to the CCR, an unauthorised disclosure of personal data occurred. This is within the scope of Article 4(12) of the GDPR.

9. BN-19-4-487

6.34 On 26 April 2019, BOI submitted a personal data breach notification to the DPC, noting that a customer was reported to the ICB and the CCR in error. BOI stated the incident occurred as a result of system inadequacies at the time of the event.

6.35 I find *BN-19-4-487* falls within the definition of a personal data breach under Article 4(12) of the GDPR. BOI's system inadequacies resulted in a breach of security leading to an unauthorised disclosure of personal data.

10. BN-19-4-490

6.36 On 26 April 2019, BOI submitted a personal data breach notification to the DPC. The notification stated that the manner in which customers' loans were restructured was reported incorrectly to the CCR. An update was given on 6 June 2019 which indicated BOI had identified additional instances of Restructure Events for mortgages not being reported correctly to the CCR. A Restructure Event is a CCR data attribute reportable where a modification is made to a credit agreement that arises from financial distress. Further updates were provided from BOI to the DPC as more errors were discovered.

6.37 The notifications can be summarised as follows. First, BOI engaged in unauthorised processing by disseminating mortgage accounts to the CCR which were out of scope because the Restructure Events had occurred prior to 30 June 2017. Second, the details of mortgage accounts that BOI reported to the CCR were inaccurately recorded where the false impression was given of some borrowers that they were in financial distress. The incidents resulted a CCR reporting error that was remedied by controls being

[19] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 8

"*implemented for manual file usage to prevent incorrect structural changes being made to files*."[20]

6.38 I find *BN-19-4-490* meets the definition of a personal data breach under Article 4(12). In reporting Restructure Events which occurred prior to 30 June 2017 BOI engaged in an unauthorised disclosure of personal data which amounts to a confidentiality breach. Reporting inaccurate personal data in respect of Restructure Events also amounts to an integrity breach.

11. BN-19-6-107

6.39 This breach notification submitted on 7 June 2019 concerned a customer who was reported to the CCR in error where they were not liable for an account since 2013. The incident arose from a manual error. New processes were subsequently implemented in relation to searches for bankrupt customers.[21]

6.40 I find this breach notification falls within the definition of a personal data breach under Article 4(12) as BOI engaged in an unauthorised disclosure of personal data which amounts to a confidentiality breach.

12. BN-18-12-240

6.41 On 14 December 2018 BOI submitted a breach notification to the DPC. It stated as a result of a technical coding error, a number of CCR records had incorrect credit agreements attached to their lending profile. In a notification dated 15 March 2019, BOI said that 2344 individuals may have been affected by the issue. In total approximately 2450 data subjects were affected by the breach.

6.42 I find *BN-18-12-240* meets the definition of a personal data breach under Article 4(12). The coding error amounted to breach of security which led to the alteration of personal data.

13. BN-19-1-203

6.43 On 18 January 2019, BOI made a breach notification to the DPC stating BOI loaded five loans to incorrect BOI customers on the CCR due to an incorrect customer ID that was included on the file. This incident resulted from inadequate technical measures, such as inadequate pre-submission checks.[22]

6.44 I find that *BN-19-1-203* meets the definition of a personal data breach under Article 4(12) of the GDPR as the customers' personal data was altered by incorrectly adding loans on customers' CCR profiles due to inadequate technical and organisational measures.

14. BN-19-2-362

[20] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 10
[21] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 11
[22] Final Inquiry Report, [227]

6.45 On 22 February 2019, BOI submitted a breach notification to the DPC that a data subject's details were mistakenly uploaded to the CCR. The data should not have been uploaded as the account was closed and the data subject was not liable for any outstanding debts. The Final Inquiry Report found that inadequate accuracy measures were in place at the time of the breach.[23] New processes were put in place "*to ensure that the source data system for reporting is updated to reflect when customers have completing a personal insolvency arrangement*."[24]

6.46 I find *BN-19-2-362* falls within the definition of a personal data breach under Article 4(12) due to BOI mistakenly altering and uploading inaccurate data for a customer to the CCR.

15. BN-19-3-364

6.47 On 22 March 2019, BOI submitted a breach notification to the DPC. The notification stated that details of a customer's loan account which was previously settled was uploaded to the CCR in error showing a debt outstanding. The incident was caused by "*inadequate procedures in place in relation to how settled accounts were reported to the CCR*."[25]

6.48 I find *BN-19-3-364* meets the definition of a personal data breach under Article 4(12) of the GDPR due to BOI mistakenly altering and uploading inaccurate data for a customer to the CCR.

16. BN-19-3-416

6.49 On 25 March 2019, BOI submitted a breach notification to the DPC. The notification stated that details of a customer's loan account which was previously settled was uploaded to the CCR in error showing a debt outstanding. This incident is a repeat occurrence of the previous incident as described under *BN-19-3-364*. BOI stated this event was caused by system inadequacy at the time of the event in the form of "*inadequate procedures in place in relation to how settled accounts were reported to the CCR*."[26]

6.50 I find *BN-19-3-416* meets the definition of a personal data breach under Article 4(12) of the GDPR due to BOI mistakenly altering and uploading inaccurate data for a customer to the CCR.

17. BN-19-4-130

6.51 On 5 April 2019, BOI submitted a breach notification to the DPC. The notification stated that details of one individual's credit card account which was previously settled was reported to the CCR incorrectly showing a debt balance and an incorrect settlement date. In subsequent notifications, BOI made clear the incident affected four individuals.

[23] Final Inquiry Report, [234]
[24] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 14
[25] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 15
[26] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 16

6.52 I find *BN-19-4-130* meets the definition of a personal data breach under Article 4(12) of the GDPR due to BOI making an unauthorised and inaccurate disclosure of personal data to the CCR. The incident resulted from a breach of security in the form of "*inadequate procedures in place in relation to how settled accounts were reported to the CCR*."[27]

18. BN-19-4-152

6.53 On 5 April 2019, BOI submitted a notification relating to the processing of inaccurate data between BOI and both the CCR and the ICB. The details of this notification mirror the details of the previous notification *BN-19-4-130* that was submitted on the same day. The notification stated details of one individual's credit card account which was previously settled was reported to the ICB and the CCR in error due to system inadequacies.

6.54 I find that *BN-19-4-152* meets the definition for a personal data breach under Article 4(12) of the GDPR. Sending details of settled credit card balances was out of scope of BOI's reporting obligations and thus amounted to an unauthorised disclosure of personal data to the CCR.

19. BN-19-5-74

6.55 On 3 May 2019, BOI submitted a breach notification to the DPC on the grounds of BOI failing to issue correspondence to mortgage customers over a period of time in advance of amending their CCR and ICB records. In a subsequent communication to the DPC dated 21 June 2019, BOI said the cases were currently under review to ascertain if the ICB and CCR records had to be amended. In a further update dated 18 November 2019, BOI stated that the event affected 810 individuals. BOI stated '*[s]ince the event was identified Bank of Ireland are no longer reporting inaccurate information to the ICB/CCR however we await confirmation that the individual records have been corrected.*' A technical fix was subsequently applied to correct the error including an automating control to monitor the creation of new folders or the deletion of existing folders.[28]

6.56 It can be deduced from this that prior to the original breach notification being made to the DPC, BOI disclosed inaccurate information relating to customers to the ICB and the CCR. I find *BN-19-5-74* falls within the definition of a personal data breach under Article 4(12) of the GDPR.

20. BN-19-5-294

6.57 On 17 May 2019, BOI submitted a breach notification to the DPC in relation to processing between BOI and both the CCR and the ICB. The notification described that as a result of a manual error a loan relating to two individuals was not restructured correctly. On 9 July 2019, BOI advised that following a further investigation it wished to withdraw the breach notification on the grounds that it established that the accounts relating to data subjects were reported correctly to the ICB and the CCR.

[27] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 17
[28] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 19

6.58 I therefore find that *BN-19-5-294* does not meet the definition of a personal data breach under Article 4(12) of the GDPR.

21. BN-19-5-296

6.59 This breach notification is similar to *BN-19-5-294.* BOI submitted a notification to the DPC on 17 May 2019 relating to inaccurate personal data being transferred from BOI to the CCR and the ICB. After conducting an investigation into the matter on 9 July 2019, BOI communicated to the DPC that the accounts relating to these data subjects had been reported correctly to the CCR and the ICB.

6.60 I therefore find that *BN-19-5-296* does not amount to a personal data breach under Article 4(12) of the GDPR.

22. BN-19-6-495

6.61 On 27 June 2019, BOI submitted a breach notification to the DPC. This notification related to one customer's loan repayments which were not correctly administered on the CCR and ICB record. The incident arose as a result of a manual error, which was subsequently addressed through the updating of training.[29]

6.62 I find that *BN-19-6-495* amounts to a personal data breach under Article 4(12) of the GDPR. As a result of BOI incorrectly altering the customer's profile inaccurate personal data was shared with the CCR and the ICB.

7. Issue 1: Article 33 of the GDPR

7.1 Article 33 of the GDPR delineates the circumstances where a controller is required to notify a personal data breach to the supervisory authority. Article 33(1) of the GDPR requires the controller to notify a personal data breach to the supervisory authority '*without undue delay and, where feasible, not later than 72 hours after having become aware of it*'. However, a controller is not required to notify the breach to the supervisory authority where it '*is unlikely to result in a risk to the rights and freedoms of natural persons*.' Where a notification is not made within 72 hours, the controller is required to give reasons for this. The importance of being able to identify a breach, assess the risk to individuals and notify it promptly is emphasised in Recital 85, which provides that:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons*".

7.2 Article 33(3) prescribes the minimum amount of detail that should make up the content of the notification. Article 33(4) states: "*[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.*" Article 33(5) requires a controller to "*document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.*"

[29] Appendix D.12 to Final Inquiry Report, Appendix 1, Row 22

7.3 The Breach Notification Guidelines address the issue of controller "*awareness*" and, in this regard, states as follows:

"*…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.* ***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.***"[30]

7.4 In this respect, the issue of controller "*awareness*", and its role in terms of defining the timeframe within which notification is required to take place, must be understood in the context of the broader obligation on a controller to ensure that it has appropriate measures in place to facilitate such "*awareness*". This requirement is reflected in Recital 87, which provides that:

"*It should be ascertained whether all appropriate technical and organizational 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…*"

7.5 Similarly, the Breach Notification Guidelines state that:

"*the 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*."

7.6 In interpreting Article 33(1) of the GDPR, it 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 of the GDPR. Regard can be had to these obligations in determining the point the controller should have been 'aware' of the existence of a personal data breach for the purposes of Article 33 of the GDPR.

[30] Breach Notification Guidelines, page 11. Emphasis added.

1. BN- 18-11-134

7.7 BOI became aware of this breach on 24 October 2018 and notified the DPC on 9 November 2018. This was 16 days after BOI became aware of the breach. In the breach notification form BOI said the breach related to economic or financial data. In an email dated 21 November 2018, BOI said as a result of a manual error a number of customers were uploaded to the CCR database that should not have been uploaded. When asked to explain the reason why the notification was not submitted within the 72 hour period prescribed by Article 33(1) or without undue delay, BOI stated:

"*An initial operational error was identified. On further investigation and during remediation of this error, the Bank became aware it also impacted the associated customer CCR record which had not been considered at the time the original error was identified.*"

7.8 In further submissions dated 5 March 2021 BOI stated:

"*We acknowledge that the Draft Report identifies several instances where our T&OMs fell short. In particular, in the following incidents, BOI's organisational measures in relation to the recording of errors on BOI's RADAR system and the subsequent risk assessment and DPC reporting process was not followed. This resulted in BOI not submitting notifications to the DPC within the 72 hours period required by Article 33 GDPR.*"

7.9 As highlighted above, the Breach Notification Guidelines make clear a controller is required to have technical and organisational measures in place which will allow establish immediately whether a personal data breach has taken place. In this case, BOI attributes inadequate organisational measures as the reason for not reporting the personal data breach within 72 hours of discovering it on 24 October 2018. I therefore find BOI has infringed Article 33(1) by failing to report the personal data breach without undue delay.

7.10 I also find BOI infringed Article 33(3) of the GDPR by failing to describe the "*nature of the personal data breach*" with the required level of precision. It will not suffice to say (as BOI did here) that personal data was uploaded to the CCR in error and that personal data included economic data. This cursory description is insufficient for the purposes of Article 33(1) GDPR.

2. BN-19-1-25

7.11 The personal data breach occurred on 9 November 2018. The breach was detected by the controller on 12 December 2018. A breach notification was made to the DPC on 4 January 2019 which was 23 days after the controller became aware of the breach.

7.12 BOI gave reasons for the delay in the breach notification form and in the response to the Commencement Letter. In response to the Commencement Letter, BOI stated:

"*At the time of identifying the error, the impact relating to the use of personal data was not identified. At the time the error was discovered, the Bank understood the error related to company accounts only however upon investigation it was subsequently*

identified there was an impact on a number of individuals. It was at this point that the Bank notified the DPC."

7.13 In a further update dated 29 January 2019 BOI stated:

"*Due to an error in how the selection criteria for a small group of non-ROI borrowers was derived, these borrowers were erroneously included in Central Credit Register (CCR) reporting. This error has been corrected and the records have been deleted from the CCR.*"

7.14 The CCR includes the credit data of business and non-business customers. Therefore, once BOI realised it had updated incorrect details to the CCR, it should have been readily apparent to BOI that it may have engaged in an unauthorised disclosure of personal data, and it should have been confirmed as soon as possible whether the error had affected personal data in consumer accounts. Nevertheless, even if BOI was ignorant of there being an unauthorised disclosure of personal data to the CCR at the date of discovery of the breach on 12 December 2018, if BOI had appropriate technical and organisational measures in place it should have been able to identify that there had been a personal data breach.

7.15 I accordingly find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

3. BN-19-1-31

7.16 A breach notification was made in respect of this breach to the DPC on 4 January 2019. In that notification BOI said the date of the incident was given as '*12 January 2018 to present*'. BOI said however it only became aware of the issue on 2 January 2019.

7.17 According to BOI, it only became aware of the breach 355 days after the incident began. 225 of those days were during the period of application of the GDPR (25 May 2018 to 4 January 2019). This is an inordinate period of time. As mentioned above, Article 33(1) must be interpreted in accordance with other obligations of the controller under the GDPR such as the obligation on the controller to demonstrate accountability under Article 5(2) and the requirement to have appropriate technical and organisational measures in place for processing. The nature of the breach was sensitive as it related to customers who were previously removed from mortgage accounts. It was incumbent on the bank to have technical and organisational measures in place which would have allowed it detect the breach at an earlier point. The failure to have such measures in place could have had negative consequences for the customers in that they could be denied credit on account of an incorrect lending history.

7.18 Accordingly, my view is that it is unsustainable for 2 January 2019 to be the date of awareness for the personal data breach under Article 33(1) of the GDPR. BOI should have been in a position to detect the breach in a shorter period than 225 days.

7.19 I therefore find that BOI has infringed Article 33(1) by failing to report the breach without undue delay.

4. BN-19-1-267

7.20 This personal data breach initially arose on 14 November 2018. BOI said it became aware of the issue on 22 January 2019. This was 69 days after the breach occurred. BOI then submitted a personal data breach notification to the DPC on 24 January 2019.

7.21 This personal data breach concerned the unauthorised disclosure of additional business credit card balances to the CCR. As a result of lenders seeing such additional balances, borrowers' opportunities to access credit from providers may have been adversely affected.

7.22 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures.

7.23 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

5. BN-19-3-33

7.24 As I found this was not a personal data breach, I also find that Article 33(1) of the GDPR was not infringed.

6. BN-19-4-117

7.25 In the breach notification form BOI submitted to the DPC, BOI noted the breach occurred on an unspecified date in 2019. BOI said it became aware of the breach on 4 April 2019 and BOI notified the breach to the DPC on the same date. This personal data breach related to inaccurate and unauthorised reporting of records to the CCR where data subjects were wrongly characterised as 'Sole Traders'. BOI subsequently, in its submissions dated 5 March 2021, noted that the actual date of discovery was 12 March 2019 instead of 4 April 2019. It follows that BOI reported the personal data breach 23 days after it became aware of the breach. BOI gave this update in light of conducting a further review and fact-check of its records.

7.26 I find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach to the DPC without undue delay.

7. BN-19-4-302

7.27 The personal data breach began on 14 November 2018 and the bank became aware of the issue on 20 December 2018. The matter was subsequently notified to the DPC on 12 April 2019, which was 113 days after BOI became aware of the breach. The breach related to a number of customer accounts which were reported to the CCR in error. These accounts were out of scope of CCR reporting as the loans had been repaid prior to the effective date of CCR reporting.

7.28 I find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

8. BN-19-4-410

7.29 The personal data breach began on 11 January 2019 and the bank became aware of the matter on 16 April 2019. The matter was notified to the DPC on 18 April 2019, which was 97 days after the personal data breach occurred. The personal data breach related to over-reporting of data subjects that had been declared bankrupt or who had exited a personal insolvency arrangement.

7.30 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures.

7.31 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

9. BN-19-4-487

7.32 The personal data breach began on 13 August 2018 and the bank became aware of the breach on 26 April 2019. The matter was notified to the DPC on 26 April 2019, which was 256 days after the personal data breach began. In the breach notification, the only details BOI gave in relation to the nature and the subject matter of the breach was that the incident occurred due to "*system inadequacies at the time of the event*" and that a customer was reported to the ICB and CCR in error (the customer notifying BOI of the event).

7.33 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures.

7.34 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

7.35 Article 33(3)(a) requires the controller in a breach notification to the DPC to describe at least "*the nature of the personal data breach*". Article 33(3)(c) requires the controller to describe "*the likely consequences of the personal data breach*".

7.36 I find BOI has infringed Article 33(3) of the GDPR by failing to provide the requisite detail required in relation to the nature of the breach or the likely consequence of the breach. Such detail is necessary to gauge the seriousness of the breach.

10. BN-19-4-490

7.37 The breach began on 10 January 2018 and BOI said it became aware of the issue on 26 April 2019. BOI notified the breach to the DPC on 26 April 2019 which was 471 days after the personal data breach began. 337 of those days were during the period of application of the GDPR (25 May 2018 to 26 April 2019). This was a substantial breach which affected approximately 47,000 data subjects.

7.38 BOI ought to have been aware of the personal data breach at an earlier stage. If BOI had adequate technical and organisational measures in place it would have been able to detect the breach at an earlier point in time.

7.39 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

11. BN-19-6-107

7.40 The personal data breach notification noted the breach began on the 24 June but no year was specified. BOI noted the date of awareness was 21 May 2019. I therefore assumed the personal data breach began on 24 June 2018 for the purposes of the Draft Decision subject to receiving submissions from BOI to the contrary. As BOI did not include any submissions to the contrary in their submissions of 2 February 2022, I conclude that the personal data breach began on 24 June 2018. BOI notified the personal data breach to the DPC on 7 June 2019, which was 348 days after the breach occurred and 17 days after BOI became aware of the breach. When asked to explain why the matter was not notified within 72 hours or without undue delay, BOI stated "*the matter was under investigation*."

7.41 I find BOI has infringed Article 33(1) of the GDPR by not notifying the DPC within 72 hours of the breach.

12. BN-18-12-240

7.42 This personal data breach occurred on 9 November 2018 and BOI said it became aware of the breach on 12 December 2018. BOI notified the breach to the DPC on 14 December 2018, two days after becoming aware of it. This was a substantial data breach which affected approximately 2450 data subjects.

7.43 I find that BOI has not infringed Article 33(1) of the GDPR in the manner in which it reported the personal data breach. It reported the breach within 72 hours after becoming aware of the breach and its date of awareness is reasonable in the circumstances.

13. BN-19-1-203

7.44 The breach occurred on 9 January 2019. BOI became aware of the breach on 15 January 2019. BOI reported the personal data breach on 18 January 2019 which appeared to be within the 72 hour period required by Article 33(1) of the GDPR.

7.45 Considering the short period of time between when the breach occurred and the point at which BOI became aware of the breach and the fact BOI appeared to have reported the breach within 72 hours of becoming aware of it to the DPC, I find BOI has not infringed Article 33(1) of the GDPR in respect of this breach.

14. BN-19-2-362

7.46 This breach occurred on 13 July 2018 and BOI said it became aware of the breach on 21 February 2019. BOI became aware of the breach following the receipt of a complaint by a data subject. BOI notified the breach to the DPC on 22 February 2019. This was 224 days after the personal data breach occurred.

7.47 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures.

7.48 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to report the personal data breach without undue delay.

15. BN-19-3-364

7.49 The breach arose on 30 June 2017 and BOI said it became aware of the matter on 5 March 2019. The breach was reported to the DPC on 22 March 2019 which was 17 days after BOI became aware of the breach. In the personal data breach notification form BOI gave the following as a reasons for the delay "*[i]nternal error. The delay was due to an ongoing investigation into this event.*"

7.50 I find BOI has infringed Article 33(1) of the GDPR in failing to notify the DPC without undue delay and within 72 hours of becoming aware of the breach.

16. BN-19-3-416

7.51 This breach began on 1 June 2017 (BOI confirmed this in an update given to the DPC on 28 June 2019). BOI said it became aware of the incident on 22 March 2019 and it notified the DPC on 25 March 2019 which was within 72 hours of the date it became aware. This breach remained undetected from the time at which the GDPR came into effect on 25 May 2018 until 22 March 2019 which was a period of 301 days. The breach related to an individual's loan account which was previously settled and was uploaded to the CCR in error.

7.52 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures. A period of 301 days is an inordinate period of time to discover a personal data breach considering the state of the art and the resources of the controller.

7.53 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to notify the DPC without undue delay of the personal data breach.

17. BN-19-4-130

7.54 The breach began on 26 April 2018. BOI said it became aware of the breach on 2 April 2019 and it was reported to the DPC 72 hours from the date BOI became subjectively aware of the breach. This breach remained undetected from the time at which the GDPR began to apply on 25 May 2018 until 2 April 2019 which was a period of 312 days. This breach related to two individuals' credit card accounts which were previously settled being reported to the CCR in error showing a debit balance and an incorrect settlement date.

7.55 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures. A period of 312 days is an inordinate period of time to discover a personal data breach considering the state of the art and the resources of the controller.

7.56 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to notify the DPC without undue delay of the personal data breach.

18. BN-19-4-152

7.57 This breach began on 11 June 2018 and BOI said it became aware of the issue on 3 April 2019. BOI notified the matter to the DPC on 5 April 2019. It took BOI 296 days to become aware of the personal data breach. This breach related to details of one individual's credit card account which was previously settled being reported to the ICB and the CCR in error due to system inadequacies.

7.58 BOI ought to have been aware of the personal data breach at an earlier stage through the implementation of adequate technical and organisational measures. A period of 296 days is an inordinate period of time to discover a personal data breach considering the state of the art and the resources of the controller.

7.59 I therefore find BOI has infringed Article 33(1) of the GDPR by failing to notify the DPC without undue delay of the personal data breach.

19. BN-19-5-74

7.60 The breach began on 3 January 2017 and BOI became aware of the issue on 23 April 2019. The breach was notified to the DPC on 3 May 2019. This was 10 days after BOI became aware of the breach. The breach related to BOI disclosing inaccurate customer data to the ICB and the CCR. BOI failed to give a detailed expression for why there was a delay in notifying the personal data breach to the DPC. BOI submitted "*this was reported outside the 72 hours as event was under investigation*." Investigating personal data breaches is not an adequate reason to not comply with reporting obligations under Article 33 of the GDPR.

7.61 I find BOI has infringed Article 33(1) of the GDPR by failing to notify the DPC without undue delay of the personal data breach.

20. BN-19-5-294

7.62 As I found this was not a personal data breach, I also find that Article 33(1) of the GDPR was not infringed.

21. BN-19-5-296

7.63 As I found this was not a personal data breach, I also find that Article 33(1) of the GDPR was not infringed.

22. BN-19-6-495

7.64 The breach began on 7 February 2019 and BOI stated the date of awareness was 21 June 2019. The breach was submitted to the DPC on 27 June 2019, which was 6 days after BOI became aware of the breach. When asked to explain why the matter was not notified within 72 hours or without undue delay, BOI stated "*this remains under*

investigation". This personal data breach related to one customer's loan repayments which were not correctly administered on the CCR and ICB record.

7.65 I find BOI has infringed Article 33(1) of the GDPR by failing to notify the personal data breach to the DPC within 72 hours of becoming aware of it and without undue delay.

Findings

7.66 I find BOI has infringed Article 33 in respect of adhering to its reporting obligations in respect of 17 personal data breaches reported. The infringements varied in respect of each personal data breach. Article 33(1) was infringed in respect of a number of personal data breaches by the BOI's failure to report the personal data breach without undue delay. Article 33(3) was also infringed by the BOI's failure to provide the information required by the Article in respect of some personal data breaches.

8. Issue 2: Article 34 of the GDPR

8.1 Article 34(1) of the GDPR states:

"*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*"

8.2 A key issue in this Decision is whether BOI was required to send a communication to data subjects in respect of any of the personal data breaches identified above on the grounds the breach was "*likely to result in a* ***high risk*** *to the rights and freedoms of natural persons*".[31] Recital 86 states a purpose of this is to allow the data subject "*to take the necessary precautions*". Determining whether any of the personal data breaches met the '*high risk*' threshold is integral to determining whether Article 34(1) is engaged in respect of any of the breaches BOI reported to the DPC.

8.3 The level of risk associated with any particular breach can be gauged with respect to the possible damage data subjects may suffer. Recital 85 gives examples of different types of damage a data subject may suffer as a result of a personal data breach:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"

8.4 The Breach Notification Guidelines emphasise the importance of taking the following factors into consideration when assessing the risk to persons arising from a personal data breach:

[31] Emphasis added.

"*Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.*"[32]

8.5 Specific factors that should be had regard to in assessing risk include:

a. The type of breach;
b. The nature, sensitivity, and volume of personal data;
c. Ease of identification of individuals;
d. Severity of consequences for individuals;
e. Special characteristics of the individual;
f. Special characteristics of the data controller;
g. The number of individuals affected.[33]

8.6 In determining if BOI has infringed Article 34(1) of the GDPR consideration must also be given to Article 34(3). Article 34(3) lists a number of conditions, any one of which may exempt BOI from having to send a communication to each data subject, even if there is a high risk to such data subjects' rights and freedoms.

1. BN- 18-11-134

8.7 In the personal data breach notification form BOI said personal data relating to 51 data subjects was provided to the CCR in error. This personal data included economic data relating to data subjects. As I have noted above BOI did not provide further detail which would allow me as decision-maker to gauge the likely risk that data subjects would incur as a result of this breach.

8.8 However, I am satisfied in light of BOI indicating in the personal data breach notification form that they have contacted the affected individuals in relation to the breach that BOI has not infringed Article 34(1) of the GDPR in respect of this breach.

2. BN-19-1-25

8.9 As was already discussed above, BOI waited a considerable period of time to notify the personal data breach to the DPC, once BOI was aware that the breach had occurred. BOI in its submissions to the DPC in respect of the draft Inquiry Report dated 6 December 2019 said: "*At the time of identifying the error, the impact relating to the use of personal data was not identified. At the time the error was discovered, the Bank understood the error related to company accounts only however upon investigation it was subsequently identified there was an impact on a number of individuals.*"

8.10 BOI should have been cognisant from an earlier stage of the possible risks to the data subjects as a result of making an unauthorised disclosure of personal data in respect of customers resident in the UK who were out of scope for the purposes of CCR reporting. The data subjects could have suffered a number of adverse consequences as a result of the breach. Any of the Credit Information Providers who had access to the CCR could

[32] The Breach Notification Guidelines, page 24.
[33] Ibid, pages 24-26.

view these customers' credit history and potentially use this as a basis to refuse loans to such customers if they intended to apply for such assistance in the future. As of 13 December 2021, 584 lenders were listed as Credit Information Providers. The volume of lenders which could access BOI's customers' credit history increases the risk of adverse consequences being suffered by data subjects' whose personal information was incorrectly disclosed.

8.11 BOI ultimately concluded the 13 affected data subjects did not need to be notified due to low risk of impact on these individuals. Having given regard to the relatively small volume of individuals affected and the fact that the customers affected were less likely (on account being resident in the UK) to apply for credit from the Irish lenders listed as Credit Information Providers, I find the personal data breach was not likely to result in a high risk to data subjects and BOI was not under an obligation to communicate the breach to them.

3. BN-19-1-31

8.12 BOI identified that this personal data breach posed a "*high*" risk to the rights and freedoms of data subjects. I agree that this was a correct characterisation of the risk considering the high volume of data subjects affected by the breach and the possibility of these data subjects suffering adverse consequences as a result of inaccurate information related to them being uploaded to the CCR.

8.13 As of 11 April 2019, BOI had communicated the personal data breach to all 197 customers affected. In determining BOI's compliance with Article 34 of the GDPR it is important to determine whether BOI contacted data subjects without undue delay.

8.14 Recital 86 states that once it has been identified the personal data breach poses a high risk to the rights and freedoms of data subjects "*[s]uch communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority*".

8.15 Considering BOI subjectively became aware of the personal data breach on 2 January 2019 and from this point had to take a number of measures including identifying the affected accounts and customers and the impact of each breach on each customer,[34] I find BOI has met its obligation to communicate the breach to data subjects without undue delay.

4. BN-19-1-267

8.16 BOI became aware of the breach on 22 January 2019 and in notifying the breach to the DPC on 24 January 2019, BOI said the risk to data subjects was "*high*". In an update received on 28 June 2019, BOI revised the total number of affected data subjects to 236. On 14 November 2019, BOI confirmed that a technical fix had now been applied to its

[34] Recital 86 of the GDPR states '*the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication*.' The latter scenario is more applicable here.

systems and it estimated that it would provide a communication to the affected data subjects by the end of November 2019. BOI confirmed on 5 December 2019 that all of the affected individuals had been notified.

8.17 From the updates BOI provided, BOI was aware of the identities of most affected individuals on 28 June 2019. However, BOI waited until 5 December 2019 to communicate the breach to the customers after a technical fix had been applied to resolve the issue. This was over 10 months after BOI became aware of the issue and 5 months after establishing the revised number of impacted individuals.

8.18 Once a high risk is identified BOI is under an obligation to communicate the personal data breach to customers without undue delay. It is particularly important in this case as such customers were susceptible to suffering economic disadvantage in credit applications from lenders who had access to the CCR on account of an inaccurate credit history being listed. If the breach had been communicated to data subjects they could have taken steps to mitigate the consequences such as explaining to prospective lenders that the CCR record did not give an accurate reflection of their creditworthiness. Alternatively, the customers could have taken steps of their own accord to remediate their CCR profile rather than waiting for BOI to apply a technical fix.[35] It is inexplicable why BOI waited until November or December 2019 to communicate the breach to individuals, when this could have been done at the end of June 2019.

8.19 I therefore find BOI has infringed Article 34(1) of the GDPR in failing to communicate this personal data breach without undue delay to the data subjects affected.

5. BN-19-3-33

8.20 As I found this was not a personal data breach, I also find that Article 34 of the GDPR was not infringed.

6. BN-19-4-117

8.21 BOI became aware of this breach on 12 March 2019. BOI identified the risk as "*high*" for the data subjects affected. I agree with BOI's assessment of this risk. As a result of company and partnership debt being wrongly attributed to individuals there was a real risk these individuals could have suffered economic disadvantage by being denied credit from lenders who had access to the CCR. BOI was aware of the identities of the affected individuals on 7 June 2019. Despite this there was a delay in communicating the breach to the majority of the affected individuals until 15 August 2019 and this process was not completed for the remaining 112 data subjects until 6 December 2019.

8.22 I find BOI has infringed Article 34(1) of the GDPR by failing to notify the affected data subjects of the breach without undue delay. Considering the high risk posed to data subjects, once BOI became aware of the breach, it should have issued communications to data subjects.

[35] For example, a data subject can complete a "*Request an Amendment Application Form*": https://www.centralcreditregister.ie/media/1431/amendment-request-application-form-en.pdf.

7. BN-19-4-302

8.23 This personal data breach concerned a disclosure of accounts with a balance of zero which had been fully repaid. This disclosure of personal data would not provide a lender who has access to the CCR with a basis to deny extending credit to any of the individual account holders.

8.24 I therefore find this personal data breach did not result in a high risk to the rights and freedoms of data subjects and BOI was not under an obligation to communicate the breach to the individuals in question.

8. BN-19-4-410

8.25 BOI became aware of this breach on 16 April 2019. BOI categorised the risk to individuals affected in the personal data breach notification form to the DPC as "*high*". BOI was aware of the identities of some of the 316 affected individuals on 2 August 2019. The breach was communicated to the individuals affected on 16 October 2019.

8.26 The first issue to consider is whether the personal data breach is likely to result in a "*high risk*" to the rights and freedoms of the individuals affected by the breach. This threshold will be met where there is a high risk the affected individuals could suffer economic disadvantage as a result of the breach.

8.27 I find that the personal data breach does create a high risk to data subjects affected. As a result of the unauthorised disclosure of persons who have exited bankruptcy or insolvency to the CCR, banks would have notice of creditors' financial histories which they may have not otherwise obtained. Following from this information being included on the CCR, lenders may rely on the individuals' credit history to deny credit to such individuals.

8.28 The second issue to consider is whether the personal data breach was communicated without undue delay to the data subjects. Considering that BOI was aware of the identities of the affected individuals who were affected by the personal data breach on 2 August 2019, it is inexplicable why BOI waited until 16 October 2019 to contact the individuals.

8.29 I therefore find BOI has infringed Article 34(1) of the GDPR by failing to contact the data subjects without undue delay.

9. BN-19-4-487

8.30 Due to the lack of information provided by BOI in respect of the nature of the breach it is difficult to make an assessment on the severity of the breach. However, considering that the breach notification form said the potential consequences of the breach for individuals was a loss of control over their personal data and damage to their reputation and that the form declared the breach to pose a "*high risk*" for data subjects, my view is that the obligation arises under Article 34 to communicate the breach to data subjects.

8.31 Although BOI had notice of the issue from a customer complaint, BOI has not

demonstrated that it sent a subsequent notification to the data subject with the information specified in Article 34(2) of the GDPR.

8.32 I find BOI has infringed Article 34(1) of the GDPR by failing to communicate the information specified in Article 34(2) to the data subject without undue delay.

10. BN-19-4-490

8.33 This personal data breach concerned "*Restructure Events*"[36] incorrectly being added to CCR customers' profiles. Many "*Restructure Events*" should not have been reported to the CCR as these "*Restructure Events*" predated CCR reporting. It was also the case that "*Restructure Events*" were incorrectly added to some customer profiles which gave a false impression that borrowers were in financial distress. The initial breach notification said one individual was affected but it ultimately transpired approximately 47,000 data subjects were affected by this breach.

8.34 BOI identified the breach as posing a "*high risk*" to data subjects. I agree with this assessment. As a result of the personal data breach the affected individuals' creditworthiness would be reduced from the perspective of a prospective lender.

8.35 BOI said it became aware of the personal data breach on 26 April 2019 but at this point had failed to ascertain the number of data subjects affected by the breach. BOI only began communicating the breach to the individuals affected in the week beginning 16 November 2020 at a rate of 7,500 data subjects per week.

8.36 A striking aspect of this personal data breach was the length of time BOI took to ascertain the volume of data subjects affected by the breach. BOI gave numerous updates to the DPC since discovering the breach on this issue. I will summarise the relevant updates below as follows:

- On 26 April 2019, BOI said one personal data subject was affected.
- On 6 June 2019, BOI said 20,000 agreements had been incorrectly submitted to the CCR as of the end of July and August 2017 and 5,000 agreements were sent with incorrect details since 30 September 2017.
- On 28 June 2019 a further update was given stating that 25,000 agreements would require amendment and the investigation remains underway to determine the final number of impacted customers.
- On 10 July 2019, BOI said it had identified approximately 42,000 individuals who were affected by the event.
- On 18 November 2019, BOI said the number of individuals affected was approximately 55,000.
- On 6 September 2019, BOI said the revised number of impacted individuals was circa 52,000.

[36] BOI defines "*Restructure Events*" as '*a CCR data attribute reportable where a modification is made to a credit agreement that arises from financial distress*.'

- On 6 March 2020, BOI said the final number of impacted individuals remained under investigation.
- On 18 June 2020, BOI said for the mortgage related error 27,453 accounts were affected. BOI said the number of customers in scope for the non-mortgage reporting error remains under investigation.
- On 17 November 2020, BOI said for the non-mortgage reporting error circa 20,000 accounts were affected. BOI said it would subsequently provide an update on the total number of individuals affected but this appears to be the last update on the number of data subjects affected by the breach.

8.37 The above timeline shows that it took BOI over a year and a half from the date of first becoming aware of the breach to provide the DPC with a final update on the number of individuals affected. BOI never provided a final number for the number of data subjects affected by the non-mortgage related error. A final number for the data subjects affected by the mortgage related error was provided for on 18 June 2020.

8.38 I find BOI has infringed Article 34(1) of the GDPR in respect of this personal data breach. Although, I acknowledge the complexity of the process in trying to ascertain the number of data subjects affected by this breach, BOI nonetheless failed to communicate the breach to data subjects without undue delay. I will outline a number of flaws in BOI's process which resulted in this infringement.

8.39 First, BOI was culpable in the length of time it took to identify the number of individuals affected by the breach. BOI should have had a quicker remediation plan which would allow it to more quickly identify individuals and thus facilitate earlier communication to the data subjects.

8.40 Second, BOI was culpable in not sending a communication to data subjects at the point it had certainty about the individuals who were affected. For example, on 18 June 2020 BOI was aware of the number of accounts affected by the mortgage related error and it was inexplicable why BOI waited until 16 November 2020 to begin to send communications to data subjects.

8.41 Third, BOI was culpable in failing to provide communications to data subjects until the errors had been remediated. BOI could have helped to avert the risk of damage to data subjects by notifying them of the breach in advance, as customers could have had regard to this if any difficulties arose in any credit applications as a result of incorrect data on the CCR.

8.42 Fourth, BOI erred in postponing sending communications until it had clearly established the total number of individuals affected by the breach. Considering the scale of the personal data breach, there will likely be a delay in arriving at this total figure. However, once BOI was certain that particular individuals had been affected by the breach and if BOI had established their identities, BOI was under an obligation to send a communication to such individuals. This was the case even if further investigations

needed to be undertaken to establish the total number of individuals affected by the breach.

11. BN-19-6-107

8.43 This personal data breach concerned inaccurate financial and economic data relating to one individual being disclosed to the CCR. BOI was subjectively aware of the identity of the affected individual on 21 May 2019. As the risk to the rights and freedoms of the data subject was assessed to be "*high*", BOI was obliged to communicate the breach to the affected individual without undue delay.

8.44 In submissions dated 5 March 2021 in respect of the Draft Inquiry Report, BOI requested that the Inquiry Report note that BOI had reduced the "*High*" risk rating to "*Low*".[37] BOI gave the following reasons for requesting the change:

"*A 'Low' risk rating means that while there was inaccurate data reported to the CCR, BOI contacted the customer promptly, no credit issues were identified by BOI or raised by the customer following those communications and the inaccurate data was rectified quickly on the CCR.*"

8.45 Even though the risk to the data subject did not materialise in this case (for example the data subject being denied credit on account of the CCR profile) it does not diminish the fact that this personal breach was likely to result in a high risk to the rights and freedoms of the data subject. In interpreting Article 34(1) of the GDPR, the test is not whether the personal data breach has caused damage to the data subject, but rather whether "*it is likely to result in a high risk to the rights and freedoms*" of the data subject. I find at the time the breach occurred this threshold was met.

8.46 My view is that BOI did not send the communication to the data subject without undue delay. Even accounting for the fact that BOI did not have a telephone number on record for the data subject, failing to contact the data subject until 12 June 2019, when the bank was aware of the risk on 21 May 2019, amounted to an undue delay. As the bank had a postal address on record a letter could have been quickly dispatched to the data subject describing the nature of the breach and any steps the data subject could take to mitigate possible effects of the breach. In particular, considering there was only one data subject affected by this breach, it is reasonable to expect there to be little delay in sending the communication.

8.47 I therefore find that BOI has infringed Article 34(1) of the GDPR by failing to send a communication to the data subject regarding the personal data breach without undue delay.

12. BN-18-12-240

8.48 For this personal data breach, BOI assessed the potential risks to the rights and freedoms of the affected individuals as "*high*" which would trigger the requirements under Article 34(1) of the GDPR to provide a communication of any personal data breach to the

[37] See pg 44 of Inquiry Report. Considered this in relation to other breaches. Solution footnote saying reasoning above also applies to other breaches to avoid duplication.

affected individuals without undue delay (unless the exception under Article 34(3) of the GDPR applied).

8.49 I agree with the assessment that the personal data breach was likely to result in a high risk to the rights and freedoms of data subjects. In an email dated 14 December 2018, BOI noted the breach resulted in an "*incorrect mortgage account number, product type, financed amount, outstanding balance, status of the borrowing e.g. existing debt, write-off debt etc*" being generated on a customer's CCR report. The high risk was borne out by two cases where customers applied for credit with BOI and the inaccurate data was included on their credit report.

8.50 BOI initially advised that there were 2,890 affected data subjects. The number of affected data subjects was higher than the number of CCR records impacted as some CCR records affected more than one person (by recording the mortgage details of other individuals). Subsequently, in a breach notification form BOI revised the number of data subjects affected by this breach to circa 1530 individuals. BOI provided a subsequent update on 29 January 2019, stating that the correct number of impacted customers was 1499 customers as a number of records did not upload to the CCR.

8.51 On 24 June 2019, a subsequent update was provided by BOI to the DPC. BOI confirmed 1391 individuals had been affected by the issue of an additional mortgage being appended to their CCR record in error (121 of these individuals are deceased). In addition, BOI confirmed 1238 individuals were affected by the issue of their mortgage agreement being no longer included in the CCR record (125 of these individuals are deceased).

8.52 The DPC contacted BOI on 21 December 2018, querying whether BOI had put a process in place for notifying the affected individuals, considering BOI had classified the personal data breach as posing a high risk to data subjects. BOI acknowledged the email on the same day but did not give an update as to notification processes. A subsequent email was sent by the DPC on 22 January 2019, seeking clarification on the latest position with regard to notifying the affected individuals. BOI confirmed on 15 March 2019 that it has issued formal letters to 2344 individuals to date.

8.53 I find BOI has not infringed Article 34(1) of the GDPR in respect of this personal data breach. Although the personal data breach was likely to result in a high risk to the rights and freedoms of individuals BOI by communicating with the data subjects on 15 March 2019 fulfilled its obligation to communicate without undue delay. Considering the volume of personal data subjects affected by the breach, BOI issued the communication within a reasonable time period.

13. BN-19-1-203

8.54 This personal data breach concerned five loans which were appended to incorrect BOI customers on the CCR. BOI classified the risks to the rights and freedoms of the affected individuals as "*low*". My view is that BOI erred in classifying this personal data breach as posing a "*low*" risk to data subjects. Uploading an inaccurate credit profile to the CCR

could result in a customer being denied credit from any of the lenders who had access to the CCR. I therefore find the personal data breach was likely to result in a "*high*" risk to the data subjects affected. This finding is not affected by the fact that no enquiries were subsequently made against these customers for the period of the error and that the customers were ultimately not adversely affected by the breach, for example, by being denied access to credit. At the time the breach was detected, such a high risk did exist and it was incumbent on BOI to contact the data subjects without undue delay.

8.55 I find BOI has infringed Article 34(1) of the GDPR by failing to contact the affected individuals without undue delay.

14. BN-19-2-362

8.56 This personal data breach related to the sharing of inaccurate financial and economic data of a customer with the ICB and the CCR. BOI became aware of the issue through a customer complaint and BOI initially assessed the risk as "*high*" on the personal data breach notification form.

8.57 BOI in its submissions dated 5 March 2021 in respect of the Draft Inquiry Report stated that it reduced the risk rating from *"High*" to "*Low*". BOI gave the following reasons for its approach:

"While there was inaccurate information reflected on the customer's ICB profile, based on our experience as a lender utilising CCR data as part of a credit assessment process, there was a low likelihood of the customer being negatively impacted in any lending decision given the nature of the error."

8.58 My view is that this personal data breach did pose a "*high risk*" to the customer's rights and freedoms. This is suggested by the fact the customer complained of the issue. If that customer sought to obtain credit from a lender who had access to the CCR, the customer may be adversely affected on account of the inaccurate information.

8.59 Although BOI had notice of the issue from a customer complaint, BOI has not demonstrated that it sent a subsequent notification to the data subject with the information specified in Article 34(2) of the GDPR.

8.60 I find BOI has infringed Article 34(1) of the GDPR by failing to communicate the information specified in Article 34(2) to the data subject without undue delay.

15. BN-19-3-364

8.61 This personal data breach related to a loan account which was previously settled being uploaded to an individual's profile on the CCR in error showing a debt outstanding.

8.62 BOI initially identified the risk as "*high*" on the breach notification form, but also sought to reclassify the breach as posing a "*low*" risk in its submissions dated 5 March 2021. I agree with BOI's initial assessment of the risk. At the time BOI identified the risk level, the borrower could have suffered adverse consequences through being denied credit from a Credit Information Provider on account of inaccurate financial information

being included on the borrower's CCR record. I find the personal data breach constituted a "*high*" risk for the purposes of Article 34(1) of the GDPR.

8.63 BOI communicated the personal data breach to the individual on 8 April 2019. This amounts to an undue delay considering BOI became subjectively aware of the breach on 5 March 2019. Considering only one individual was affected it was inexcusable for BOI to wait until 8 April 2019 to send the communication to the data subject.

8.64 I find BOI has infringed Article 34(1) of the GDPR by failing to communicate the breach without undue delay to the customer.

16. BN-19-3-416

8.65 This personal data breach related to details of an individual's loan account which was previously settled being uploaded to the CCR in error. This incident is a repeat occurrence of a previous incident described under BN-19-3-364.

8.66 For the same reasons given in the previous incident, I agree with BOI's initial assessment of the risk as "*High*" and that it should not be reclassified as "*Low*" for the purposes of Article 34(1).

8.67 The data subject contacted the bank on 22 March 2019 notifying it of the issue. BOI has not demonstrated that it sent a subsequent notification to the data subject with the information specified in Article 34(2) of the GDPR.

8.68 I find BOI has infringed Article 34(1) of the GDPR by failing to communicate the information specified in Article 34(2) to the data subject without undue delay.

17. BN-19-4-130

8.69 This personal data breach related to details of four individuals' credit card accounts which were previously settled being uploaded to the CCR in error which incorrectly showed a debt balance and an incorrect settlement date. On 5 April 2019, in the breach notification made to the DPC BOI submitted that the incident affected one individual. This was revised to two individuals on 8 May 2019. This was revised to four individuals on 7 June 2019. BOI stated that two individuals had made contact with the bank to report inaccuracies in their own CCR records.

8.70 On 28 June 2019, BOI stated that the inaccurate data relating to customers had been remediated. However, in its submissions in respect of the Draft Inquiry Report dated 5 March 2021, BOI stated "*the records were not amended until 14 December 2020 and not as originally thought in June 2019.*"

8.71 BOI assessed the risk to the individual as "*High*". I agree with this assessment as it related to the sharing of inaccurate sensitive personal data. This personal data breach was likely to result in a high risk of the individuals in question being denied credit by lenders who had access to the CCR.

8.72 I find BOI has infringed Article 34(1) of the GDPR by failing to communicate the information required by Article 34(2) after becoming aware of the personal data breach. This communication was particularly important in respect of this personal data breach considering the inaccurate data was not remediated for a considerable period of time.

18. BN-19-4-152

8.73 On 5 April 2019, BOI submitted a notification relating to the processing of inaccurate data between BOI and both the CCR and the ICB. The details of this notification mirror the details of the previous notification *BN-19-4-130* that was submitted on the same day. The notification stated details of one individual's credit card account which was previously settled was reported to the ICB and the CCR in error due to system inadequacies.

8.74 BOI became aware of the breach on 3 April 2019. BOI confirmed that the lending record was purged by both the CCR and the ICB on 15 April 2019.

8.75 BOI initially classified the risk the data breach posed to the individual as "*high*". I agree with this assessment as the individual may have suffered adverse consequences in future applications from credit as a result of the breach.

8.76 Following on from this personal data breach, BOI did not send a communication to the individual affected. I do not see any reason why it was not reasonably feasible to send a communication to the data subject on this issue.

8.77 I therefore find BOI has infringed Article 34(1) of the GDPR by failing to send a communication to the data subject without undue delay.

19. BN-19-5-74

8.78 BOI became aware of the issue on 23 April 2019 and a breach notification was made to the DPC on 3 May 2019. The breach related to BOI disclosing inaccurate customer data to the ICB and the CCR. BOI categorised the risks to the rights and freedoms of the individuals as "*high*". It ultimately transpired 810 individuals had been affected by the breach.

8.79 It took BOI a considerable period of time to investigate the personal data breach. In an update which was received by the DPC on 28 June 2019, BOI confirmed that as of 21 June 2019, it was still determining to what extent the alterations put in place by BOI affected CCR records. In an update dated 21 June 2019, BOI said once the cases have been reviewed to establish if there is a requirement to amend the ICB/CCR record, BOI will be writing to all the affected customers advising them of the error and confirming that the ICB/CCR record will be amended accordingly.

8.80 On 18 November 2019, BOI provided an update to the DPC that 694 individuals had been notified about the event. On 28 May 2020, in an update to the DPC BOI said it had advised all data subjects about the breach with the exception of five individuals. BOI said it was researching up to date contact information for the remaining customers and

was awaiting confirmation from the CCR and ICB that the affected records had been corrected. BOI subsequently confirmed it had contacted all the individuals affected by the breach apart from one individual. BOI did not have up to date address details for this data subject and attempts to contact the individual by phone were unsuccessful.

8.81 I find BOI has infringed Article 34(1) of the GDPR by failing to contact the data subjects affected without undue delay. I acknowledge that in this case it would not have been reasonably feasible for BOI to contact the individuals affected immediately after the bank became subjectively aware of the breach due to the scale of the breach. Nonetheless, I find BOI has infringed Article 34(1) by failing to contact 694 individuals affected until 18 November 2019 which was 6 months and 26 days after it became aware of the breach. BOI delayed sending communications to the data subjects until it had received confirmation that the CCR record was amended. BOI erred in this regard, as BOI's duty to communicate to data subjects arises once a high risk to the rights and freedoms of customers has been identified following the breach.

8.82 The fact that the remainder of the customers affected (with the exception of one individual) were only contacted on 28 May 2020 also amounts to an undue delay. This was over a year since BOI became aware of the breach and it could be expected BOI would have been able to trace the contact details of customers at a more expeditious rate. I find BOI has infringed Article 34(1) by failing to communicate the breach to data subjects without undue delay.

20. BN-19-5-294

8.83 As I found this was not a personal data breach, I also find that Article 34(1) of the GDPR was not infringed.

21. BN-19-5-296

8.84 As I found this was not a personal data breach, I also find that Article 34(1) of the GDPR was not infringed.

22. BN-19-6-495

8.85 On 27 June 2019, BOI submitted a breach notification to the DPC. This notification related to one customer's loan repayments which were not correctly administered on the CCR and ICB record. BOI said it became aware of the breach on 21 June 2019. BOI categorised the breach as posing a "*high*" risk to the customer affected. I agree with this assessment as the risk to the customer of being denied credit in future applications was heightened by incorrect financial data being included on the CCR and the ICB register.

8.86 I find BOI has infringed Article 34(1) of the GDPR in respect of this breach. Despite categorising this breach as posing a "*high*" risk to the data subject, BOI has not demonstrated that it sent the required communication to the data subject without undue delay.

9. Issue 3: Article 32 of the GDPR

9.1 In considering BOI's obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk under Article 32 of the GDPR, I have taken into account BOI's submissions in respect of the Draft Inquiry Report.[38] In particular, I have given regard to BOI's submission "*that it will not be realistically possible for BOI (or any Credit Information Provider within the meaning of the CRA 2013) to operate a zero error model*." I have also given regard to BOI's emphasis on Article 5(1)(d) of the GDPR which states (emphasis added) "*[p]ersonal data shall be… accurate and where necessary, kept up to date ;* ***every reasonable step*** *must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay…*"[39]

9.2 Although, in this part of the Decision I am analysing BOI's compliance (or lack thereof) with Article 32 of the GDPR, I accept that Article 32 should be interpreted in light of other Articles of the GDPR such as Article 5. I accept BOI's submission that Article 32 of the GDPR will not automatically be infringed if an incident occurs which renders personal data inaccurate. Rather, in considering whether the requirements of Article 32 have been met by the controller, it is necessary to assess whether the controller has adequately gauged the level of risks to data subjects and whether the controller has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The different factors listed in Article 32(1) should be taken into account when carrying out this assessment. If a controller has correctly identified the risks and has implemented appropriate security measures there will be no infringement of Article 32 of the GDPR, even if personal data has been rendered inaccurate. However, in practice, many personal data breaches occur as a result of a lack of appropriate technical and organisational measures in place.

9.3 Article 32(1) of the GDPR elaborates on the requirement in Article 5(1)(f) to provide for the security of processing:

'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;

[38] Appendix 11 Submissions 5 March 2021.
[39] Emphasis added.

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

9.4 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.

i. Assessing Risk

9.5 The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the processing. Article 32(2) of the GDPR expressly states that the risks of alteration or unauthorised disclosure should be considered when assessing the appropriate level of security. Regarding BOI's processing of personal data, a risk of alteration includes sensitive customer personal data being mistakenly altered due to a system error or a manual human error. A risk of an unauthorised disclosure includes sharing personal data with third parties where BOI does not have authority to do so or sharing inaccurate customer data with third parties.

9.6 Recital 76 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.*"

9.7 It is necessary to carry out an objective assessment of the risks presented by the processing to determine the appropriate level of security. Risk must be assessed by reference to (i) the likelihood of the risk, and (ii) the severity of the risk to the rights and freedoms of natural persons. In BOI's case, this risk assessment must have particular regard to ensuring the integrity and accuracy of personal data of customers on its systems. The risk assessment should also have particular regard to the risk of unauthorised disclosure to third parties, whether that is by disclosing accurate data without the requisite authority or disclosing inaccurate customer data.

9.8 Regarding the nature, scope, context and purposes of BOI's processing of personal data, as outlined above, the nature of BOI's processing is sensitive. Its scope is extensive. Section 11 of the 2013 Act places an obligation on lenders to provide personal and credit information for qualifying credit applications where the credit applied for exceeds €500. S.I. No. 486/2016 gives examples of information which must be provided for different credit arrangements including "*Restructure Events*", "*Payment Made Date*" and "*Outstanding Balance*".[40] The context for sharing the data is BOI's statutory obligations under the 2013 Act. The purpose of the processing is to have a centralised register of borrowers from which lenders can assess their creditworthiness.

[40] S.I. No. 486/2016 - Credit Reporting Act 2013 (Section 11) (Provision of Information for Central Credit Register) Regulations 2016.

9.9 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[41] provides guidance as to the factors that should inform this risk assessment. In the case, the CJEU declared the Data Retention Directive[42] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to (i) the vast quantity of data retained, (ii) the sensitive nature of the data, and (iii) the risk of unlawful access. In assessing the risk posed by BOI's processing, regard must also be had to these factors.

9.10 BOI processes a vast quantity of personal data on data subjects. According to BOI's website, BOI serves 2 million consumer and business customers across a broad range of segments and sectors.[43] BOI is under a statutory obligation to disclose many of its customers' personal data to the CCR which involves a substantial amount of data processing. BOI in its submissions in respect of the Draft Inquiry Report said it submits data to the CCR for over 1 million contracts and 1 million customers on a monthly basis.

9.11 The personal data processed by BOI is sensitive in some instances. The data includes information about borrowers' financial histories which varies from credit card debts, mortgage repayments, periods of personal insolvency and bankruptcy, and details of any restructuring events on the customers' accounts.

9.12 There is a significant risk of BOI incurring a breach of security as a result of its processing operations. As is evident from the personal data breaches identified in the Inquiry, BOI's processing includes the transfer of personal data to the CCR (and in some cases the ICB before it was wound up). The personal data that can be disclosed to the CCR depends on what categories of personal data fall under the scope of the 2013 Act. Technical and organisational measures BOI has for ensuring the integrity/accuracy of personal data and for ensuring that only personal data within the scope of BOI's reporting obligations is disclosed, play an integral role in protecting the rights and freedoms of data subjects. In these circumstances, there is a high risk of unlawful access to personal data in the absence of appropriate technical and organisational measures to ensure the integrity of personal data and to prevent the unauthorised disclosure of such.

9.13 I find that BOI's processing of personal data in relation to the CCR presents a high risk, both in likelihood and severity, to the rights and freedoms of natural persons. The risk to the rights and freedoms of natural persons manifests itself, in particular, in the risk of

---

[41] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl* and others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

[42] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[43] < https://investorrelations.bankofireland.com/about-us/bank-of-ireland-overview/> accessed on 30th November 2021.

unlawful or unauthorised disclosure to third parties. Such risks include disclosing personal data to the CCR which is outside the scope of BOI's reporting obligations or disclosing inaccurate personal data to third parties. The likelihood of such risks occurring must be categorised as high due to the quantity of data processed and how that processing includes transferring personal data to third parties.

9.14 The severity of the risk to the rights and freedoms of natural persons arising from such unlawful or unauthorised disclosure is also high. The high severity of this risk flows from the sensitive nature of the personal data that is processed and the context and purposes of the processing. BOI processes sensitive economic and financial information which it discloses to the CCR pursuant to obligations under the 2013 Act. Any lenders listed as "Credit Information Providers" are able to access the CCR for the purpose of assessing the creditworthiness of prospective borrowers. There are high risks to data subjects if BOI discloses inaccurate personal data or personal data which is outside the scope of its reporting obligations to the CCR as borrowers could be denied access to credit as a result of this information. This could result in "*financial loss… or any other significant economic or social disadvantage*" to natural persons which is a type of damage envisaged by Recital 75 of the GDPR. Thus the severity of the risk is also high.

iii. Security measures implemented by BOI

9.15 The first personal data breach reported by BOI to the DPC is *BN 18-11-134.* The incident occurred on 12 October 2018. Although a number of breaches reported by BOI first occurred in 2019, the majority first occurred in 2018. I will have regard to these timeframes in assessing what were the appropriate technical and organisational measures BOI ought to have had in place when the breaches occurred.

9.16 On 21 February 2020, the DPC wrote to BOI to enquire *inter alia* what technical and organisational measures it had in place at the time the personal data breaches took place to comply with Article 32 of the GDPR. BOI responded on 28 February 2020. BOI said the technical and organisational measures in place at the time of the breach included: User Acceptance Testing, Day 1-10 runbook checks pre-submission of the monthly files, monthly review of customer complaints to review/identify any CCR trends and any errors occurring.

9.17 BOI also said it adopted a Quality Assurance approach which includes reporting of key performance indicators, management information, evaluation checks to management to implement plans to rectify weaknesses. In addition there is bank agent call monitoring with customers and BOI provides Information Security, Data Management and Data Protection and Privacy training. BOI also has user access management controls on its system.

9.18 Other measures mentioned by BOI include IT Service Continuity tests, Business Continuity Plan supported by an IT Service Continuity Recovery Plan and Crisis Management Governance Model documents. BOI said these plans are tested annually.

iv. Appropriate Security Measures

i) Security measures to preserve accuracy of the data

9.19 BOI ought to have implemented robust validation procedures prior to transferring personal data to the CCR or the ICB. BOI has responsibility to verify the accuracy of the personal data and to ensure the personal data sent is within the scope of BOI's reporting obligations prior to disclosing it to the CCR or the ICB. This would help to eradicate coding errors which resulted in personal data breaches.[44] If BOI had robust validation measures in place, it would have helped it to detect design failures in its disclosure system which would have helped it to pre-empt certain personal data breaches.[45] There was also a lack of quality assurance controls and oversight mechanisms to ensure appropriate procedures were followed. I find BOI has failed to implement robust validation procedures and quality assurance controls. I have given regard to the state of the art and the costs of implementation and I am of the view these would be appropriate technical and organisational measures to adopt.

9.20 BOI ought to have implemented a means of clearly distinguishing between personal data that it was required to report to the CCR under the 2013 Act and personal data that was out of scope in its CCR reporting solution. A number of personal data breaches resulted from BOI's failure to have an adequate taxonomy in place.[46] An appropriate measure could be reporting flags which BOI implemented subsequent to some personal data breaches taking place. I find BOI has failed to implement appropriate security measures such as reporting flags to ensure only personal data within the scope of BOI's reporting obligations was disclosed to the CCR. I have given regard to the state of the art and the costs of implementation and I am of the view this would be an appropriate technical and organisational measure to adopt.

9.21 An appropriate security measure to implement is training for staff responsible for making transfers to the CCR on how to properly fulfil their obligations. I have given regard to the state of the art and the costs of implementation and I am of the view this would be an appropriate technical and organisational measure to adopt. I note BOI in submissions to the DPC has included copies of CCR training materials for staff.[47] I note the majority of the training materials were delivered in 2019 which was after the period in which many personal data breaches occurred. BOI has supplied two training packs for training which took place in 2018.[48] The training delivered in March 2018 focuses

[44] See for example BN-18-12-240.

[45] See for example BN-18-11-134.

[46] See for example BN-19-1-25, BN-19-1-31 and BN-19-1-267.

[47] Asset Finance, CCR Enquiry Training (August 2019); Central Credit Register, Training Pack – CCR Enquiry for BBLS & SME LA's (January 2019); Central Credit Register, Training Pack – CCR Enquiry for Corporate Banking (January 2019); Central Credit Register, Multi-Bureau – Refresh Guide Cards, Overdrafts & Personal Loans (December 2018); BB Comms CCR Reminder May 19; BB Comms CCR Update Mar 19; CCR Training Pack – Consumer Customer Query Handling (March 2018), CCR Manual Solution FAQ & Errors Handling (August 2019); MARS & ROIC Radar Errors and Events Training Q1 2019 (29 March 2019); and Guide to the CCR Consumer Credit Report March 18 included in Appendix 4 BOI Submissions 6 December 2019.

[48] CCR Training Pack – Consumer Customer Query Handling (March 2018) and Central Credit Register, Multi-Bureau – Refresh Guide Cards, Overdrafts & Personal Loans (December 2018) included in Appendix 4 BOI Submissions 6 December 2019.

on the period in the aftermath of a personal data breach occurring rather than on how to prevent a personal data breach occurring in the first place. The second training delivered in December 2018 is more comprehensive. It focuses on the importance of inputting personal data accurately the first time. I find this is an appropriate security measure. However, I find BOI did not have adequate training in place for staff on how to prevent personal data breaches between 25 May 2018 (the date on which the GDPR came into effect) and December 2018 when the second training was delivered. It is important to emphasise that BOI has an ongoing obligation to provide appropriate data protection training to staff. Generic training will not suffice to fulfil BOI's obligations under Article 32. The training delivered must be continually re-evaluated in line with advancements in the state of the art and it should incorporate lessons learned from previous mistakes.

9.22 BOI in its submissions also acknowledged there was a lack of Subject Matter Experts involved at the design stage.[49] I welcome that BOI's submission that it has dedicated more '*subject matter experts to ensure greater technical detail is captured for development and design purposes for CCR reporting.*'

ii) Technical and organisational measures to identify the breach promptly and to rectify it

9.23 It took BOI a considerable period of time to identify many of the personal data breaches which are the subject of this Decision. Developing an inferred view of the CCR database is an appropriate security measure to assist BOI in identifying personal data breaches, and therefore, in implementing an appropriate level of security. I have given regard to the state of the art and the costs of implementation and I am of the view this would be an appropriate technical and organisational measure to adopt. If a customer makes a complaint to BOI, having an inferred view of the database enables BOI to more proactively respond to the customer's complaints and also facilitates the identification of similar errors. BOI noted prior to developing such a system it had no sight of the CCR system and this seemed to contribute to the delay in discovering and remedying the personal data breaches. I find BOI did not have such a security measure in place at the time the personal data breaches occurred. However, I welcome the fact that BOI has developed such a database as of the first quarter of 2020.

9.24 I have taken into account BOI's submission that it is outside BOI's power to unilaterally fix errors on the CCR register.[50] BOI is dependent on the Central Bank to adopt these fixes on notification and this sometimes results in an inevitable delay. Although, there will be a delay on account of being dependent on a third party, BOI is nonetheless required to adopt technical and organisational measures to ensure errors are remediated quickly insofar as it is in its power to do so.

9.25 I welcome BOI's submission that it has installed a process which allows for large scale amendments of the CCR register which is made possible due to the existence of the bespoke inferred view database.[51] I have given regard to the state of the art and the costs

[49] See for example BN-19-4-490.
[50] Appendix 11. Submissions 5 March 2021 in respect of Draft Inquiry Report paragraph 9.10.
[51] Appendix 11. Submissions 5 March 2021 in respect of Draft Inquiry Report paragraph 9.10.

of implementation and I am of the view this would have been an appropriate technical and organisational measure to adopt at the time the personal data breaches occurred. This process will enable BOI to amend errors in the CCR record without delay. I find BOI did not have such a process in place at the time the breaches occurred.

9.26 I note as of 10 April 2019, BOI has an Error Management Procedure in place which, if followed, will allow BOI to expeditiously identify personal data breaches.[52] This is an appropriate technical and organisational measure for the purposes of Article 32 of the GDPR. However, I could find no such error management procedure in place at the time the majority of the personal data breaches occurred**.** I therefore find BOI did not have such a procedure in place prior to 10 April 2019.

iii) Technical and organisational measures to identify customers affected by the breach and to ensure prompt communication if necessary

9.27 BOI in its submissions to the DPC, included copies of data protection training it provided to staff.[53] These documents, among other things, emphasise the importance of reporting data incidents within 24 hours on BOI's Radar platform to facilitate the DPO reporting any personal data breaches to the DPC within 72 hours of becoming aware of the breaches. BOI also provided copies of training documents for staff responsible for CCR reporting.[54]

9.28 The training materials, however, fail to emphasise the importance of communicating to individuals affected by the personal data breach where it has been determined that the breach is likely to result in a high risk to the rights and freedoms of individuals. Having given regard to the state of the art and the costs of implementation, I find this is an appropriate security measure to adopt and I find BOI did not incorporate such a procedure.

9.29 It is my view that BOI has also failed to demonstrate that it has a clear procedure in place which outlines who is responsible for issuing a communication to data subjects where a personal data breach is likely to result in a high risk to their rights and freedoms.

Findings

9.30 I find that BOI infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level security appropriate to the risk presented by its processing of customer data in transferring information to the CCR.

[52] Appendix 4 BOI Submissions 6 December 2019 page 187.

[53] See Data Protection & Privacy Event Management Overview September 2018; Bank of Ireland 2019 Data Protection and Privacy Regulatory Engagement Back 2 Basics; 2019 Group Data Protection & Privacy Training included in Appendix 4 BOI Submissions 6 December 2019.

[54] Asset Finance, CCR Enquiry Training (August 2019); Central Credit Register, Training Pack – CCR Enquiry for BBLS & SME LA's (January 2019); Central Credit Register, Training Pack – CCR Enquiry for Corporate Banking (January 2019); Central Credit Register, Multi-Bureau – Refresh Guide Cards, Overdrafts & Personal Loans (December 2018); BB Comms CCR Reminder May 19; BB Comms CCR Update Mar 19; CCR Training Pack – Consumer Customer Query Handling (March 2018), CCR Manual Solution FAQ & Errors Handling (August 2019) and MARS & ROIC Radar Errors and Events Training Q1 2019 (29 March 2019) included in Appendix 4 BOI Submissions 6 December 2019.

10. Decision on Corrective Powers

10.1 I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that BOI infringed Articles 33, 34 and 32 of the GDPR. 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. The remaining question for determination in this Decision is whether or not those infringements merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

10.2 Recital 129 of the GDPR, which acts as an aid to the interpretation of Article 58, provides that '*... each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case ....*' In the circumstances of the within Decision, and with particular reference to the findings arising therefrom, I find that the exercise of one or more corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR.

10.3 Having carefully considered the infringements, I have decided to exercise corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringements in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2). In summary, the corrective powers that I have decided to exercise are:

a. Article 58(2)(b) – I have decided to issue a reprimand to BOI for its infringements of Articles 32, 33 and 34 of the GDPR.

b. Article 58(2)(d) – I have decided to order BOI to bring its processing operations into compliance with Article 32 in the terms set out below.

c. Article 58(2)(i) – I have decided to impose administrative fines pursuant to Article 83, in respect of a number of BOI's infringements of Article 33 and Article 34. I have also decided to impose an administrative fine for BOI's infringement of Article 32 of the GDPR.

A. Reprimand

10.4 I issue BOI with a reprimand in respect of its infringements of Articles 33, 34 and 32 of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to '*issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation.*' It is my view that a reprimand is appropriate, necessary and proportionate in view of ensuring compliance with the Articles I have found were infringed in this Decision. It is clear from the GDPR that reprimands do not have to be issued in isolation to the exercise of any other corrective powers. Furthermore, each measure that I am imposing by way of the exercise of a corrective power for the infringements I have found must be appropriate, necessary and proportionate in view of ensuring compliance with the GDPR. In this respect, I consider

it appropriate, necessary and proportionate to impose reprimands in addition to the order and administrative fines detailed below in order to give full effect to the obligations in Articles 33, 34 and 32 and to formally recognise the seriousness of the infringements found in this Decision.

10.5 On 2 February 2022, BOI submitted that reprimands should not be issued for the infringements of Articles 33 and 34 provisionally identified in the Draft Decision. They highlighted that it had been decided not to issue a reprimand for infringements of Articles 33(1) and 33(5) in a Decision dated 9 December 2020 with case reference IN-19-1-1 (the "**Twitter Decision**"), due to a "*stateable*" argument that, on the basis of the wording in Article 58(2)(b) of the GDPR, reprimands cannot be issued for infringements that do not comprise "*processing operations*." In the Twitter Decision, there was no definitive conclusion on the meaning and effect of the phrase "*processing operations*" as it appears in Article 58(2)(b).[55]

10.6 "*Processing operations*" is not a defined term in the GDPR, but "*processing*" is defined in Article 4(2) of the GDPR as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*." Notifying data subjects of a personal data breach necessarily involves the processing of personal data, and the obligations under Article 34 therefore necessitate "*processing operations*" as understood within the context of the Article 58(2)(b).

10.7 It also appears that while "*processing*" is a subset of "*processing operations*," the concept of "*processing operations*" is broader than the concept of "*processing*." In the Twitter Decision, it was noted that "*It is, therefore, arguable that, in the context of a breach notification under Article 33(1), given that a breach is something affecting, or done to, personal data, it follows that the notification obligation (insofar as it inherently must entail an examination of what has happened to personal data or how it has been affected (i.e. under Article 33(1)) is intrinsically connected to one or more processing operations.*"[56] Moreover, an "*operation*," by dictionary definition means "*the fact of operating or being active*," "*the way that parts of a machine or system work together, or the process of making parts of a machine or system work together*," "*an activity that is planned to achieve something*," or, in a business context, "*the activities involved in a*

[55] The full passage at paragraph 12.5 of the Twitter Decision reads: "*At the same time, I do consider that the definition of the term "processing", within which the word "operations" appears, is very broadly construed. It is, therefore, arguable that, in the context of a breach notification under Article 33(1), given that a breach is something affecting, or done to, personal data, it follows that the notification obligation (insofar as it inherently must entail an examination of what has happened to personal data or how it has been affected (i.e. under Article 33(1)) is intrinsically connected to one or more processing operations. While I do not consider it necessary to definitively conclude on the meaning and effect of the term "processing operations" as it appears in Article 58(2)(b) for the purposes of this Decision, on balance, I consider that TIC's legal argument supporting their contention that a reprimand should not be issued in the context of infringements under Articles 33(1) and 33(5) is a stateable one. I have, therefore, decided not to proceed with the issuing of a reprimand to TIC in relation to the infringements which I have found in this Decision*."

[56] Twitter Decision, paragraph 12.5

company producing goods or delivering services."[57] Consequently, in a business or organisational context "*processing operations*" can be considered to be an organisation's overall procedures and activities relating to the processing of personal data, which is broader than the fact of processing itself. "*Processing operations*" can therefore be considered to include the handling of incidents that have an impact on personal data, such as the notification of personal data breaches to data subjects and supervisory authorities.

10.8 It is also notable that there is no reference to "*processing operations*" in relation to the power to issue administrative fines,[58] and the Recitals to the GDPR envisage a degree of interchangeability between the issuing of reprimands and administrative fines. Recital 148 states (emphasis added),

"*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***."

10.9 On the basis of this analysis, it is not inconsistent with the wording or the object and purpose of the GDPR to issue a reprimand for the infringements of Articles 33 and 34 of the GDPR identified in this Decision.

B. Order

10.10 I order BOI to bring its processing operations into compliance with Article 32 of the 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. Article 58(2)(d) 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*.' It is my view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with Article 32 of the GDPR. In this regard, I acknowledge BOI's on-going remedial actions and strategic transformation, as outlined in submissions throughout the Inquiry. However, it is my view that this order is necessary and proportionate in light of the importance of ensuring that full effect is given to BOI's obligation to implement appropriate technical and organisational measures, having particular regard to the high quantity, highly sensitive personal data of data subjects processed by BOI.

10.11 The orders I have decided to impose are set out in the following table:

Number	Action	Timescale
1.	Article 32 Lack of robust validation procedures and quality assurance controls	BOI is required to confirm to the Data Protection Commission that this order has been complied with

[57] OPERATION | meaning in the Cambridge English Dictionary (accessed 24 February 2022)
[58] See Articles 59(2)(i) and 83 of the GDPR

	I order BOI to upgrade its validation procedures in relation to verifying the accuracy of data prior to making transfers to the CCR. I order BOI to implement quality assurance controls to ensure this upgraded procedure is followed.	within 90 days of the date of this Decision.
2.	Article 32 Lack of emphasis in training materials on the importance of communicating to data subjects where a personal data breach is likely to result in a high risk to their rights and freedoms I order BOI to implement relevant training for staff relating to BOI's obligations under Article 34 of the GDPR	BOI is required to confirm to the Data Protection Commission that this order has been complied with within 90 days of the date of this Decision.
3.	Article 32 Absence of a procedure which outlines who is responsible for issuing a communication to data subjects where a personal data breach is likely to result in a high risk to their rights and freedoms I order BOI to implement such a procedure.	BOI is required to confirm to the Data Protection Commission that this order has been complied with within 90 days of the date of this Decision.

C. Administrative Fine

10.12 Article 58(2)(i) permits the DPC to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in section 115 of the 2018 Act, which permits the DPC to impose an administrative fine on its own in combination with any other corrective power specified in Article 58(2).

10.13 Article 83(1), in turn, identifies that the administration of fines '*shall in each individual case be effective, proportionate and dissuasive*'. In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) of the GDPR.

10.14 The decision as to whether to impose an administrative fines (and if so, the amount of the fines) is a cumulative decision which is taken having had regard to the factors as set out in Article 83(2)(a) to (k). Therefore, I will now proceed to consider each of these criteria in turn in respect of BOI's infringements of Articles 33, 34 and 32 of the GDPR.

(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;

i. Article 33 of the GDPR

10.15 I have found BOI has infringed Article 33 of the GDPR in relation to *BN-18-11-134, BN-19-1-25, BN-19-1-31, BN-19-1-267, BN-19-4-117, BN-19-4-302, BN-19-4-410,*

BN-19-4-487, *BN-19-4-490*, *BN-19-6-107*, *BN-19-2-362*, *BN-19-3-364*, *BN-19-3-416*, *BN-19-4-130*, *BN-19-4-152*, *BN-19-5-74* and *BN-19-6-495*.

10.16 The nature of the infringements concerned a failure by BOI to adhere to its reporting obligations under Article 33 of the GDPR. The purpose of Article 33 is to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded to the extent possible by mitigating the risks to them arising from a data breach. BOI's infringements of Article 33 arose in circumstances where it failed to report the personal data breaches without undue delay. The nature of the personal data breaches are such that they have the potential to adversely influence lending institutions' decisions on the data subjects' access to credit. By failing to notify the DPC of these personal data breaches without undue delay, BOI potentially prevented and/or delayed enforcement action from the supervisory authority which may have been appropriate in light of the risks posed by the personal data breaches. This, in turn, could have an impact on the safeguards and mitigation measures which data subjects might otherwise benefit from.

10.17 BOI's infringements of Article 33 of the GDPR in respect of the above breach notifications, particularly those in the cases of *BN-19-4-117* and *BN-19-5-74*, are grave in nature. As a result of BOI's failure to report personal data breaches to the DPC without undue delay in accordance with Article 33(1) of the GDPR the rights and freedoms of data subjects were at risk for a sustained period of time.

10.18 The purpose of the processing was to adhere to a statutory obligation imposed on BOI by the 2013 Act. The purpose of the reporting obligation stems from the legislative desire to have a centralised register of borrowers where their creditworthiness can be assessed by lenders.

10.19 The scope of the processing is to report accurate information required by the 2013 Act to the Central Bank. Insofar as BOI reported inaccurate information it has exceeded the scope of its statutory obligations under the 2013 Act.

10.20 The number of data subjects affected and the level of damage suffered by them varied in relation to each infringement of Article 33 of the GDPR. In relation to some of BOI's infringements only one data subject was affected. However, for another infringement approximately 47,000 data subjects were affected.[59] The damage caused to the data subjects as a result of the infringements included a high risk of economic or financial damage by being denied credit from lenders who had access to the CCR.

10.21 If the personal data breaches were reported earlier damage could have been averted whether that is by enabling data subjects to regain control of their personal data at an earlier stage or reducing the risk of the data subjects being adversely affected by inaccurate information when applying for credit.

[59] See BN-19-4-490.

ii. Article 34 of the GDPR

10.22I have found that BOI has infringed Article 34 of the GDPR in relation to *BN-19-1-267*, *BN-19-4-117*, *BN-19-4-410*, *BN-19-4-487*, *BN-19-4-490*, *BN-19-6-107*, *BN-19-1-203*, *BN-19-2-362*, *BN-19-3-364*, *BN-19-3-416*, *BN-19-4-130*, *BN-19-4-152*, *BN-19-5-74* and *BN-19-6-495*.

10.23The nature of the infringements concerned a failure by BOI to issue communications to data subjects without undue delay in circumstances where the personal data breaches were likely to result in a high risk to the data subjects' rights and freedoms.

10.24The infringements are of a serious gravity, particularly those arising from breach notifications *BN-19-4-490*, *BN-19-1-267*, *BN-19-4-410*, and *BN-19-5-74*. As a result of BOI's failure to communicate to data subjects, the data subjects may have been unaware of the high risk to their rights and freedoms and were not able to take steps to mitigate the consequences of the breaches. Steps the customers could have taken may have included bringing to the lender's attention that the CCR did not give an accurate account of their creditworthiness or of their own volition seeking to have the CCR profile amended.

10.25The duration of the infringements arising from each personal data breach varied, but for the purposes of the decision to impose an administrative fine, the duration of any infringement is not considered to begin until the date the GDPR began to apply on 25 May 2018. Each infringement ended on the date on which the personal data breach was communicated to the data subjects in question.

10.26The purpose of the processing was to adhere to a statutory obligation imposed on BOI by the 2013 Act. The purpose of the reporting obligation stems from the legislative desire to have a centralised register of borrowers where their creditworthiness can be assessed by lenders.

10.27The scope of the processing is to report accurate information required by the 2013 Act to the Central Bank. Insofar as BOI reported inaccurate information or information outside the scope of the 2013 Act it has exceeded the scope of its statutory obligations under the 2013 Act.

10.28The number of data subjects affected and the level of damage suffered by them varied in relation to each infringement of Article 33 of the GDPR. In relation to some of BOI's infringements only one data subject was affected. However, at the other end of the scale, for one infringement approximately 47,000 data subjects were affected.[60] The damage caused to the data subjects as a result of the infringements included a high risk of economic or financial damage by being denied credit from lenders who had access to the CCR.

[60] See BN-19-4-490.

10.29 Many data subjects were likely to have suffered damage as a result of BOI's delay in sending the communication to data subjects. If a communication had been issued to data subjects earlier, data subjects could have provided this to a prospective lender to show them that their profile on the CCR was not reflective of their creditworthiness. This could have helped to prevent data subjects suffering adverse consequences as a result of the personal data breach. The fact that BOI received a number of complaints from customers attests to the seriousness of the personal data breaches.[61]

iii. Article 32 of the GDPR

10.30 BOI's infringement of Article 32 of the GDPR includes the 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 through transferring it to the CCR. I found BOI infringed Article 32 of the GDPR by failing to implement robust validation procedures, adequate quality assurance controls, an adequate taxonomy to identify which personal data was in scope, adequate training for staff involved in the processing operations, an inferred view database, error management procedures and a procedure for communicating to data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms.

10.31 The infringement is of a serious gravity. BOI's lack of technical and organisational measures at the time of the breach contributed to inaccurate and unauthorised personal data being included on the CCR. The infringement also contributed to the delay in identifying the personal data breach and in some cases resulted in a delay in the breach being communicated to data subjects or the breach not being communicated at all.

10.32 The infringement of Article 32 has a duration from when the GDPR came into effect on 25 May 2018 and is ongoing at the date of this Decision on foot of necessary technical and organisational measures remaining to be implemented. Some technical and organisational measures have yet to be implemented by BOI, including those outlined in the order set out at 10.B above. However, it is acknowledged that BOI has taken a number of steps to update its technical and organisational measures following the personal data breaches. On 5 March 2021, BOI submitted a CCR DP Action Plan that was implemented following the findings in the Draft Inquiry Report. On 2 February 2022, BOI confirmed that all 13 action items on that plan have now been completed.

10.33 The purpose and scope of the processing carried out by BOI in respect of CCR obligations has been discussed above.

10.34 BOI's failure to implement appropriate organisational and technical measures required by Article 32 of the GDPR increased the risk profile for all of BOI's customers. Over 50,000 data subjects were affected by the personal data breaches considered in this Decision through having their personal data erroneously disclosed to the CCR. However, all of BOI's customers were affected in that the failure to have appropriate technical and organisational measures in place could have resulted in any customer (and

[61] For example, for *BN-19-4-490* BOI received approximately 323 customer complaints, of which it deemed 71 complaints required further investigation

in some cases ex-customers') personal data being erroneously disclosed to the CCR. This is evidenced by the multiple personal data breaches described in this Decision where personal data was shared despite it being outside the scope of BOI's reporting obligations.

(b) the intentional or negligent character of the infringement;

i. Article 33 of the GDPR

10.35 BOI's infringements of Article 33(1) of the GDPR were of a negligent character. BOI was negligent in failing to abide by its own policies and procedures in failing to report some personal data breaches to the DPC within 72 hours of becoming subjectively aware of the personal data breaches.

10.36 In respect of where I found that BOI ought to have been aware of the existence of the personal data breaches at an earlier point in time and consequently failed to fulfil its reporting obligations under Article 33(1) of the GDPR, BOI was negligent in failing to embed appropriate technical and organisational measures which would have enabled BOI to detect the personal data breaches at an earlier stage.

ii. Article 34 of the GDPR

10.37 The infringements were of a negligent character. If BOI had appropriate procedures and training in place communications would have been made to data subjects without undue delay.

iii. Article 32 of the GDPR

10.38 The infringements were of a negligent character. Once errors began to occur BOI took steps to prevent recurrences of the errors. The DPIA for CCR reporting did not consider the risk of inaccurate or unauthorised data being disclosed and this attests to the negligent character of the infringement.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

i. Article 33 of the GDPR

10.39 Once the personal data breaches were identified, BOI took steps to remediate the customers' records on the CCR.

ii. Article 34 of the GDPR – BN-19-4-490

10.40 BOI did ultimately send a communication to data subjects in all cases where a personal data breach posed a high risk to their rights and freedoms. However, many communications were only sent after a prolonged delay.[62]

[62] For example, for BN-19-4-490, BOI began sending communications to data subjects on the week beginning 16 November 2020. This was over 16 months after the DPC received the notification of the breach.

iii. Article 32 of the GDPR

10.41 BOI sought to mitigate the damage, by remediating the erroneous data on the CCR. After a number of personal data breaches occurred, BOI also subsequently introduced different technical and organisational measures such as reporting flags, tailored CCR training for staff, dedicating more Subject Matter Experts to designing the programme, developing an inferred view database, creating a bulk amendment facility for the CCR and creating an Error Management Procedure. As noted above, BOI confirmed that all 13 action items on their CCR DP Action Plan have been completed. Those items included:[63]

- Contacting all remaining outstanding customers impacted by the in-scope reported error;
- Error Ref BN-19-4-490 (Restructuring event) remediation of 99% of records and with approach in place to close the remaining 1%, being more complex record errors;
- Refresh and approval of Group Data Management Policy and Standards;
- Communication of enhanced Group Data Management Operating Model based on the refreshed Policy and Standards;
- Presentation of revised Data Protection Event Framework to DPC;
- Operationalise revised Data Protection Event Framework;
- Operationalise an accelerated and more proactive customer communication approach;
- Refresh CCR Reporting DPIA;
- Review of CCR reporting solution error management process to further assess and challenge remediation timelines;
- Review of existing action plans or activities underway as part of CCR Programme, as a way of further evidence adequacy of processing controls and error management;
- Mobilise a task force focused on systematic root cause analysis of business reporting errors and remediation;
- Commence data profiling and data issue identification across source systems with assigned business owners;
- Deploy T&OM enhancements and training in line with systemic root cause analysis findings and remediation.

(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;

i. Article 33 of the GDPR

10.42 BOI is responsible for failing to integrate technical and organisational measures which would have allowed BOI to become aware of personal data breaches at an earlier stage.

[63] BOI Submissions 5 March 2021, p3

ii. Article 34 of the GDPR

10.43BOI is responsible for failing to integrate technical and organisational measures which would have allowed BOI to identify customers which BOI was obliged to send a communication to under Article 34.

iii. Article 32 of the GDPR

10.44BOI is responsible for failing to implement the appropriate technical and organisational measures required by Article 32 in respect of its data processing operations at issue in this Decision. I accept, however, the view that BOI was dependent on the Central Bank to make some changes on the CCR. In their submissions on 2 February 2022,[64] BOI provided an update on the steps taken to liaise with the Central Bank to improve errors management, and I consider it appropriate to take these steps into account as a mitigating factor for the purposes of this Decision.

(e) any relevant previous infringements by the controller or processor;

i. Article 33 of the GDPR

10.45Not applicable.

ii. Article 34 of the GDPR

10.46Not applicable.

iii. Article 32 of the GDPR

10.47Not applicable.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

i. Article 33 of the GDPR

10.48BOI 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 found that BOI infringed Article 33(3) in respect of a number of breach notifications by failing to describe the personal data breaches concerned with the required level of precision.

ii. Article 34 of the GDPR

10.49BOI notified the DPC of its intended timelines to send communications to customers who fell within the scope of Article 34 of the GDPR.

iii. Article 32 of the GDPR

10.50BOI has provided particulars of where the organisation's technical and organisational measures were deficient. BOI has updated the DPC on new technical and organisational measures it has integrated since the personal data breaches occurred, including by developing the CCR Action Plan highlighted in the sections under Articles 83(2)(a) and

[64] BOI Submissions 2 February 2022, paragraph 11.1(d)

83(2)(c) of the GDPR, and has provided the DPC with updates on the progress of this plan during the investigative and decision-making stages.[65]

(g) the categories of personal data affected by the infringement;

i. Article 33 of the GDPR

10.51 The personal data affected by the infringements included sensitive financial and economic personal data from which the data subjects' creditworthiness was to be derived.

ii. Article 34 of the GDPR

10.52 The personal data affected by the infringement included sensitive financial and economic personal data from which the data subjects' creditworthiness was to be derived.

iii. Article 32 of the GDPR

10.53 The personal data affected by the infringement included sensitive financial and economic personal data from which the data subjects' creditworthiness was to be derived.

(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. Article 33 of the GDPR

10.54 I found that BOI infringed Article 33(1) of the GDPR in respect of a number of breach notifications in failing to report the existence of a personal data breach to the DPC without undue delay.

ii. Article 34 of the GDPR

10.55 BOI has provided periodic updates to the DPC on steps it has taken to remediate the personal data breaches and its timelines to issue communications to data subjects.

iii. Article 32 of the GDPR

10.56 BOI 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.

(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;

i. Article 33 of the GDPR

10.57 Not applicable.

[65] Ibid, paragraph 11.1(f)

ii. Article 34 of the GDPR

10.58Not applicable.

iii. Article 32 of the GDPR

10.59Not applicable.

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

i. Article 33 of the GDPR

10.60Not applicable.

ii. Article 34 of the GDPR

10.61Not applicable.

iii. Article 32 of the GDPR

10.62Not applicable.

(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.

10.63In their submissions of 2 February 2022, BOI requested that the DPC note that it did not gain any financial benefit from the purported infringements. This is noted.

10.64I find there are no other aggravating or mitigating factors in respect of the infringements of Articles 33, 34 and 32 of the GDPR.

i. Decision to Impose Administrative Fines

Methodology

10.65In the absence of specific EU-level guidelines on the calculation of fines, I am not bound to apply any particular methodology.[66] In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the fine. Therefore, in calculating the fine I will identify the amount of the administrative fine to be imposed on BOI on a general basis and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

10.66In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it

[66] See by analogy Case T 332/09, *Electrabel v Commission,* judgement of 12 December 2012 (ECLI:EU:T:2012:672), paragraph 228; Case T-704/14, *Marine Harvest ASA v Commission*, judgement of 26 October 2017 (ECLI:EU:T:2017:753), paragraph 450.

does not have significance relative to the financial resources of the data controller. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. This is compounded by the fact that future infringements need to be deterred. In this regard, I consider that a fine cannot be dissuasive if it will not be of any financial significance.

10.67 As regards the maximum amount for the fine that can be imposed in respect of each infringement of Article 33, 34 and 32 the relevant fining cap is the higher of €10,000,000 or 2% of the annual turnover of the preceding financial year. Therefore, I find that the cap for each of BOI's infringements is **€52.4 million**.[67] This figure is not a starting point, but rather the cap on the permitted range as provided for in Article 83(4) of the GDPR.

10.68 I will now consider whether to impose a fine for the infringements considered in relation to Article 83(2) above.

i. Article 33 of the GDPR

10.69 I have decided to impose an administrative fine for BOI's infringement of Article 33(1) in respect of *BN-19-4-117*. My view is that it is appropriate to impose an administrative fine for this infringement considering the large number of data subjects affected (approximately 420 data subjects were affected) and the inordinate delay in reporting the personal data breach to the DPC after BOI became subjectively aware of the personal data breach.[68] BOI was negligent in failing to report the personal data breach within the prescribed period. As a result of this infringement, the data subjects' rights and freedoms were at risk for a longer period than they otherwise would have been if the personal data breach was reported promptly. I consider that a fine of **€40,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

10.70 I have decided to impose an administrative fine for BOI's infringement of Article 33(1) in respect of *BN-19-5-74*. My view is that it is appropriate to impose an administrative fine for this infringement considering the large number of data subjects affected (approximately 810 data subjects were affected) and the inordinate delay in reporting the personal data breach to the DPC after BOI became subjectively aware of the personal data breach.[69] BOI was negligent in failing to report the personal data breach within the prescribed period. As a result of this infringement, the data subjects' rights and freedoms were at risk for a longer period than they otherwise would have been if the personal data breach was reported promptly. I consider that a fine of **€50,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

[67] BOI's operating income in 2020 was €2620 million (See Bank of Ireland Group plc Annual Report 2020). 2% of this figure amounts to €52.4 million. Bank of Ireland's Annual Report for 2021 was not available at the time of writing.

[68] BOI reported the personal data breach **23 days** after it became aware of the breach and outside the 72 hour time limit specified by Article 33(1).

[69] BOI reported the personal data breach **10 days** after it became aware of the breach and outside the 72 hour time limit specified by Article 33(1).

10.71 Regarding the other infringements of Article 33, I have decided not to impose administrative fines in respect of these infringements. On the particular facts of this Inquiry, I find it would not be proportionate to impose an administrative fine for these infringements of Article 33 having regard to the particular circumstances of these infringements and the general dissuasive effect of the fines imposed regarding *BN-19-4-117* and *BN-19-5-74*.

ii. Article 34 of the GDPR

10.72 Having considered the criteria set out in Article 83(2) of the GDPR, I have decided to impose an administrative fine for BOI's infringement of Article 34 of the GDPR in respect of *BN-19-4-490*.

10.73 In arriving at the decision to impose an administrative fine, I have been influenced by the length of the delay it took BOI to issue a communication to data subjects after it became aware of the personal data breach. [70] I have also had regard to the large number of data subjects which were affected by this infringement (approximately 47,000) and the number of complaints BOI received from customers. I have also taken these factors into consideration in determining the quantum of the fine.

10.74 I consider that a range of **€125,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

10.75 I have decided to impose an administrative fine for BOI's infringement of Article 34 of the GDPR in respect of *BN-19-1-267*. I have been influenced by the length of delay it took BOI to issue a communication to data subjects after it became aware of the personal data breach.[71] I have also had regard to the large number of data subjects which were affected by this infringement (approximately 236). I have also taken these factors into consideration in determining the quantum of the fine.

10.76 I consider that a fine of **€6,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

10.77 I have decided to impose an administrative fine for BOI's infringement of Article 34 of the GDPR in respect of *BN-19-4-410.* I have been influenced by the length of delay it took BOI to issue a communication to data subjects after it became aware of the personal data breach.[72] I have also had regard to the large number of data subjects

[70] BOI became aware of the personal data breach in April 2019 yet only began issuing communications in November 2020

[71] BOI became aware of the personal data breach in January 2019 yet only issued communications to data subjects in December 2019.

[72] BOI became aware of the breach in April 2019 yet only issued communications to data subjects in October 2019.

which were affected by this infringement (approximately 316). I have also taken these factors into consideration in determining the quantum of the fine.

10.78 I consider that a fine of **€6,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

10.79I have decided to impose an administrative fine for BOI's infringement of Article 34 of the GDPR in respect of *BN-19-5-74*. I have been influenced by the length of delay it took BOI to issue a communication to data subjects after it became aware of the personal data breach.[73] I have also had regard to the large number of data subjects which were affected by this infringement (approximately 810). I have also taken these factors into consideration in determining the quantum of the fine.

10.80I consider that a fine of **€11,000** is appropriate in the circumstances of this case. I consider that a fine of this amount is an effective, proportionate and dissuasive figure as required by Article 83(1).

10.81I have decided not to impose administrative fines for BOI's other infringements of Article 34(1) of the GDPR. My reasons for this are that less data subjects were affected by the other infringements of Article 34(1) and in many cases there was less of a delay in issuing communications to data subjects.

iii. Article 32 of the GDPR

10.82Having considered the criteria set out in Article 83(2) of the GDPR, I have decided to impose an administrative fine for BOI's infringement of Article 32 of the GDPR.

10.83In arriving at a decision to impose an administrative fine and the quantum thereof I have given regard to the criteria in Article 83(2) of the GDPR. In particular, I have given regard to the fact that the lack of technical and organisational measures in place manifestly contributed to the personal data breaches that occurred. I have given regard to the fact that the infringement was of a negligent character along with the steps BOI took to mitigate the damage.

10.84I consider that a fine of **€225,000** is appropriate in the circumstances of this case. I consider that a fine from this range is capable of being an effective, proportionate and dissuasive figure as required by Article 83(1).

ii. Total Value of the Administrative Fine

10.85Article 83(3) of the GDPR states:

'*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount*

[73] BOI became aware of the breach in April 2019 yet only began issuing communications in November 2019. A number of customers were not contacted until May 2020.

of the administrative fine shall not exceed the amount specified for the gravest infringement.'

10.86 In a recent decision (the "**WhatsApp Decision**"), the EDPB held that the reference to '*gravest infringement*' in Article 83(3) did not relate to gravest infringement identified in a particular inquiry, but rather referred to the fining caps referred to in Articles 83(4) and Article 83(5) of the GDPR.[74] Accordingly, as Decision Maker I am not restricted to only imposing an administrative fine for the most serious infringement of the GDPR in this case.

10.87 Considering the severity of each of the infringements of the GDPR which in my view justify the imposition of administrative fines under Article 83 and considering the requirement under Article 83(1) for the administrative fines to be imposed to be '*effective, proportionate and dissuasive*' I am of the view it is necessary to impose each of the administrative fines outlined above.

10.88 Therefore, the total value of the administrative fines that I have decided to impose is **€463,000**.

10.89 It is my view that the above administrative fines cumulatively meet the requirements of being effective, proportionate and dissuasive as required by Article 83(1) of the GDPR. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any proposed fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fines imposed do 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 fines I have decided to impose are effective, proportionate and dissuasive, taking into account all of the circumstances of the inquiry.

11. Right of Appeal

11.1 This Decision is issued 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 imposes administrative fines, BOI will also have the right to appeal against this Decision within 28 days from the date on which notice of this Decision is given to it.

Helen Dixon

Commissioner for Data Protection

[74] 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).

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

Breach Notifications with correspondence

Letter of Commencement IN-19-9-5

BOI acknowledgement of Inquiry 12 November 2019

BOI replies to Letter of Commencement 6 December 2019

DPC further enquiries 21 February 2020

BOI submissions 28 February 2020

DPC further enquiries 7 May 2020

BOI submissions 22 May 2020

BOI CCR Schematic

BOI CCR event log June 2019

BOI submissions 5 March 2021

Submitted Appendix 1 on Breach Corrective Actions

Submitted Appendix 2 on Event & Error Reporting & Management

BOI submissions 2 February 2022