In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-7-2

In the matter of Irish Credit Bureau DAC

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

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

DECISION

Decision-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

23 March 2021

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**"the Decision"**) is a decision made by the Data Protection Commission (**"the DPC"**) in accordance with Section 111 of the Data Protection Act 2018 (**"the 2018 Act"**). I make this Decision having considered the information obtained in the separate own volition inquiry (**"the Inquiry"**) conducted by a case officer of the DPC (**"the Case Officer"**) pursuant to Section 110 of the 2018 Act. The Case Officer provided the Irish Credit Bureau DAC **("the ICB")** with the Draft Inquiry Report and the Final Inquiry Report.

1.2 The ICB was provided with the Draft Decision on this Inquiry on 2 February 2021 to give it a final opportunity to make submissions. This Decision is being provided to the ICB pursuant to Section 116(1)(a) of the 2018 Act in order to give the ICB 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 (**"the GDPR")** arising from the infringements that have been identified herein. In this regard, the ICB is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on the ICB 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

2.3 The decision-making process for this Inquiry is provided for under Section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the Commission, 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 the ICB has furnished to me, and any other materials that I consider relevant, in the course of the decision-making process.

2.4 The Final Inquiry Report was transmitted to me on 10 September 2020, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and the ICB; and copies of all submissions made by the ICB, including the submissions made by the ICB in respect of the Draft Inquiry Report. The ICB made submissions on the Draft Decision on 23 February 2021. A full schedule of all documentation considered by me for the purpose of this Decision is appended hereto. I issued a letter to the ICB on 20 November 2020 to notify it of the commencement of the decision-making process.

2.5 Having reviewed the Final Inquiry Report, and the other materials provided to me by the Case Officer, including the submissions made by the ICB, 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. Factual Background

3.1 The ICB is a credit reference agency that maintains a database on the performance of credit agreements between financial institutions and borrowers (**"the ICB database"**). Approximately 280 financial institutions are members of the ICB[1] (**"ICB members"**) and those members register information on the performance of credit agreements with the ICB, usually on a monthly basis. ICB members can access the information on the ICB database by making enquiries with the ICB. The ICB also uses this information to create credit reports and credit scores in respect of borrowers. This information assists the financial institutions in making decisions on applications for credit. The credit reports form a part of the process used by financial institutions to make decisions on applications for credit. The ICB submitted that other factors play a significant role in lending decisions and that *"In ICB's experience, the same data provided from ICB can lead to different lending decisions being taken by different lenders, as they have different lending criteria and varying risk appetites."*[2]

[1] ICB "Observations & Clarifications identified in the Draft Inquiry Report (IN-19-7-2)", dated 20 August 2020.
[2] ICB submissions on the Draft Decision, dated 23 February 2021, at page 6.

3.2 ICB members are contractually obliged to update the ICB database with new data on loans. ICB members submit approximately 3.5 million monthly updates. The ICB uses an automated system for processing updates to its database. However, the ICB manually processes payment profile updates[3]. [redacted]

3.3 [redacted] The ICB implemented a filter on completed accounts [redacted] This meant that when a borrower fully repaid and completed a loan, the record of that loan on the database was un-editable and protected from erroneous updates.

3.4 On 28 June 2018, the ICB implemented a code change in order to amend how it updates a subset of payment profiles on the database (**"the code change"**). [redacted] The intention of the change was to improve the accuracy of the database by allowing those accounts to accept updates where the account holder made subsequent payments.

3.5 The code change contained a technical error. This error allowed updates to completed accounts and removed the filter that previously protected those accounts from erroneous updates. [redacted]

[3] The "ICB Members Technical Manual", dated July 2015, at page 24.
[4] The ICB provided a full list of the profile indicators was in the "ICB Members Technical Manual", dated July 2015, at page 43.
[5] Note of meeting between the DPC and the ICB on 26 October 2018 at 11am, appendix C.1 to the Inquiry Report at page 208.

3.6 Between 28 June 2018 and 30 August 2018, the ICB database inaccurately updated the records of 15,120 closed accounts resulting from the technical error (**"the personal data breach"**). The vast majority of the inaccurate updates resulted in an incorrect closure date being recorded on the ICB database to state that the closed account had closed more recently that it actually had. 18 account records had an incorrect balance applied, but none of those records were disclosed to ICB members. All of the affected accounts remained designated as completed on the system. 98.12% of the 15,120 account records were closed credit card accounts. The remainder consisted of closed mortgage, personal loans and asset finance loan accounts.

3.7 Of the 15,120 accounts affected, the ICB disclosed 1,062 inaccurate account records to its members or data subjects before fixing the issue. This figure includes 118 inaccurate credit reports disclosed directly to data subjects. All of the inaccurate account records disclosed to the ICB members stated that the accounts had been closed more recently than they actually had been, but none misstated that a balance was outstanding on the accounts.

3.8 The ICB became aware of a potential issue on 27 August 2018 when an ICB member notified it that the finalised date on a customer credit card record had erroneously changed. This change also resulted in a new credit score for the customer. The ICB investigated this matter and determined on 29 August 2018 that the code change caused the error by removing the filters on the ICB database. On 31 August 2018, the ICB fixed the validation rules that allowed the incorrect changes to closed accounts and corrected the affected data. The ICB notified 3 ICB members, whose updates accounted for 98% of incorrect account records, of the personal data breach on 31 August 2018. The ICB also notified the DPC of the personal data breach on 31 August 2018.

3.9 Following the notification of the personal data breach, the ICB cooperated with the DPC's assessment of the personal data breach. The ICB submitted a number of documents in response to the DPC's queries, as included in the appendix hereto, and I have had due regard to those documents in making this Decision. The ICB notified the remaining 20 of its members, whose updates accounted for 2% of incorrect account records, of the personal data breach on 4 and 5 September 2018. By 21 September 2018, the ICB had contacted the 130 of its members, who had not provided incorrect updates during the breach period but had accessed some of the 15,120 inaccurate records, to notify them of the breach and to provide them with encrypted copies of the inaccurate data and the restored data. The ICB also asked those members to review their lending decisions in the period and, if necessary, to contact any data subjects whose credit application may have been adversely affected by the inaccurate data. The ICB requested that those members confirm to ICB if it had been necessary to contact any data subjects. The ICB submitted that *"ICB has not been advised by any member that any of this population of data subjects had an application for credit declined because of the incorrect closure date on a closed account."*[6]

[6] ICB submissions on the Draft Decision, dated 23 February 2021, at page 10.

3.10 On 24 September 2018, the ICB notified each of the data subjects who had directly requested the 118 credit reports from ICB of the personal data breach, provided them with a new credit report, and suggested that they contact any lenders to whom they had made credit applications during the breach period if necessary.

3.11 On 19 July 2019, the DPC informed the ICB of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry (**"the Notice"**). The DPC made the decision to commence the Inquiry having regard to the circumstances of the personal data breach. The Notice set out the scope and legal basis of the Inquiry. The Notice informed the ICB that the Inquiry would examine whether or not the ICB had discharged its obligations in connection with the subject matter of the breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the ICB in that context. The Notice set out that the Inquiry would seek to establish the facts as they relate to the subject of the Inquiry. The Notice also posed a number of queries to the ICB and sought relevant documentation that informed those responses.

3.12 The ICB responded to the Notice on 15 August 2019 and answered the queries. The ICB provided an overview of its database and submitted the latest version of the ICB Members Technical Manual, which came into effect from August 2018. A previous version of the Technical Manual, dated July 2015, was in effect up until that point and is, therefore, also relevant to the period under consideration in this Decision. The ICB also outlined that it achieved the ISO27001 certification in October 2012 and that it maintains its certification with bi-annual audits from Certification Europe. The ICB also submitted a number of documents relevant to the Inquiry.

3.13 On 19 November 2019, the Case Officer wrote to the ICB with a number of follow-up queries in respect of the information provided by the ICB. The ICB responded to these queries on 3 December 2019 and submitted a range of further documents. The ICB clarified that it had assessed the risk of the code change as *"Medium"* on the change request because the change intended to affect a relatively small number of records [redacted] The ICB stated that it had no further documentation in relation to the change process or records beyond the change request and the fix already disclosed.

3.14 On 11 March 2020, the Case Officer wrote to the ICB seeking specific information on the technical and organisational measures that were in place at the time of the personal data breach to counter the risks with the forms of data processing at issue in the breach. The ICB responded to the DPC's request on 24 March 2020. The ICB also submitted that it did not test for the condition that prevented updates to closed accounts because there was no reason to specifically test for that condition. The ICB submitted that it fully logged all changes to the database in journals as standard and that this gave the ICB the ability to trace, understand, fix and recover fully within the 72-hour data breach notification period.

3.15 On 23 July 2020, the Case Officer issued the ICB with the Draft Inquiry Report and invited submissions. The Draft Inquiry Report included the relevant facts as provisionally established

by the Case Officer and the Case Officer's provisional views on the issues within the scope of the Inquiry.

3.16 On 20 August 2020, the ICB made submissions on the Draft Inquiry Report. The ICB outlined remedial steps that it was in the process of taking in response to the personal data breach, which included testing methodologies, DPIAs, and a new change control process in respect of future changes to the ICB system. The ICB also submitted details of a data remediation governance review aimed at improving its existing framework. The ICB's technical working group met almost weekly to review progress in strengthening ICB's technical and organisational measures. The submissions also made observations and clarifications on the Draft Inquiry Report, which I have considered for the purposes of this Decision.

3.17 On 10 September 2020, the Case Officer completed the Final Inquiry Report and submitted it to me as decision-maker. On 20 November 2020, I wrote to the ICB to notify it of the commencement of the decision-making stage of the Inquiry. On 14 December 2020, I wrote to the ICB requesting a copy of the *"ICB ISO Policy document"* referred to by the ICB during the Inquiry. The ICB submitted a copy of this document, titled *"A12 Operations Security"*, on 16 December 2020. I provided the ICB my Draft Decision on 2 February 2021 and the ICB was afforded the opportunity to make submissions on the proposed infringements that were provisionally identified therein and the corrective powers that I proposed to exercise. On 23 February 2021, made submissions on the Draft Decision. I have had full regard to those submissions and I have reached conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

3.18 In its submissions on the Draft Decision, the ICB outlined that during its remediation process it created new policies and processes in relation to change control and testing, and updated its existing policies and processes. The ICB had implemented 10 updated and newly created policies/processes by mid-October 2020. Following my request on 14 December 2020, the ICB provided me with one of these updated documents (*"A12 Operations Security"*). However, in its submissions on the Draft Decision, the ICB submitted that:

> *"*while highlighted in the Operations Security Policy, *the remaining nine updated and newly created policies/procedures were not specifically provided to the DPC. We apologise for omitting these documents from the DPC review as it means that in reaching the provisional views set out in the Draft Decision, unfortunately the DPC was not aware of the full extent of the remediation actions on change control and testing already implemented by ICB*."[7]

3.19 The ICB submitted that it conducted a further review and updates of all ICB policies and processes in relation to change control and testing following receipt of the Draft Decision[8]. This review resulted in further updates and newly created policies and processes. The ICB's

[7] ICB submissions on the Draft Decision, dated 23 February 2021, at page 14.
[8] Ibid.

submissions on the Draft Decision appended the original ICB change control and testing policies, the change control and testing policies post 20 August 2020, and the change control and testing policies post 2 February 2021. As outlined below, I have had due regard the ICB's full remediation process and the full suite of documents submitted in relation to the decision on corrective powers in Part 9 of this Decision.

4. Scope of the Inquiry

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine whether or not the ICB has discharged its obligations in connection with the subject matter of the personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by the ICB in that context.

4.2 In this regard, the Notice expressly stated that the scope of the inquiry would include Articles 5, 24, 25(1), 26, and 28 of the GDPR. The Notice stated that the Inquiry would focus on the areas of Data Protection Governance, Training and Awareness, Records Management, Security of Personal Data, Data Sharing, Privacy Impact Assessments, and Records of Processing Activities.

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:

(i) Whether the ICB complied with its obligation pursuant to Article 25(1) of the GDPR to implement appropriate technical and organisational measures which are designed to implement the principle of accuracy, provided for in Article 5(1)(d) of the GDPR, in an effective manner;

(ii) Whether the ICB complied with its obligations, pursuant to Articles 5(2) and 24(1) of the GDPR, to demonstrate compliance with the data protection principles and to demonstrate that processing is performed in accordance with the GDPR; and

(iii) Whether the ICB, along with the ICB members, were obliged, pursuant to Article 26(1) of the GDPR, to determine their respective responsibilities for compliance with the GDPR by means of an arrangement between them.

6. Issue 1: Article 25(1) of the GDPR

6.1 Article 25(1) of the GDPR provides for data protection by design:

> *"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and*

at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

6.2 Article 5(1)(d) of the GDPR provides for the principle of accuracy, requiring 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 ('accuracy')"

6.3 As outlined in further detail in Part 8 of this Decision, the ICB is the controller in respect of the ICB database. Therefore, pursuant to Article 25(1), the ICB is obliged, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures to implement the data protection principles, including the principle of accuracy provided in Article 5(1)(d). This must include measures to address the risk of inaccurate personal data being stored or further processed on the ICB database, and is not limited only to measures designed to rectify or erase inaccurate data where it is processed. This obligation in Article 25(1) is scalable depending on the particular circumstances of the processing undertaken and the risks presented. Therefore, in determining whether the ICB has infringed Article 25(1), it is necessary to determine which measures were appropriate at the time of the personal data breach.

6.4 The ICB faces challenges in ensuring that the personal data it processes are accurate. The ICB submitted that it takes data directly from its members and has limited opportunity to adjudicate on the accuracy of that data[9]. In *Huber v Bundesrepublik Deutschland*[10] the Court of Justice of the European Union considered the lawful basis for a centralised register of personal data. Various public bodies were authorised to enter data and information directly in the register. The Court held that *"As the authority entrusted with the management of the [register], the Bundesamt is responsible for the accuracy of the data registered in it."*[11] The obligation in Article 25(1) applies to the controller of that database. Therefore, the ICB cannot avoid its obligation under Article 25(1) simply because it relies on ICB members to submit accurate personal data. However, the assessment of what constitutes *"appropriate technical and organisational measures"* must have regard to the particular circumstances of the processing. Therefore, in considering whether the ICB has infringed Article 25(1), I must have had due regard to how the ICB relies on its members in respect of the accuracy of the personal data.

[9] ICB submissions on the Draft Inquiry Report, dated 20 August 2020, at page 2.
[10] Case C-524/06, Heinz Huber v Bundesrepublik Deutschland, judgment of 16 December 2008 (ECLI:EU:C:2008:724).
[11] At paragraph 21.

6.5 Article 25(1) also requires that the state of the art, the cost of implementation and the nature, scope, context and purposes of processing must be taken into account when implementing data protection by design. The controller must also consider the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

6.6 Turning first to the nature, scope, context and purposes of the ICB's processing of personal data on its database, I consider that the nature of this processing is inherently sensitive. The personal data concerns data subjects' performance on credit agreements. Any mishandling of this personal data, due to inaccuracy, unauthorised disclosure, or otherwise, may seriously infringe the rights and freedoms of data subjects. The ICB relies on alphanumerical sequences submitted by ICB members to update the personal data on the database. Errors in these sequences can cause inaccuracy on the database, which, in turn, can result in adverse consequences for credit applicants.

6.7 The scope of the processing on the ICB database is broad. The database records the performance of credit agreements concerning the ICB members. Those members are contractually obliged to provide regular updates to the ICB, resulting in 3.5 million monthly updates. In 2018, the ICB database contained approximately 6.7 million account records (3.2 million open loans and 3.5 million closed loans). The ICB database contains other personal data on account holders, such as their occupation, address, gender and date of birth. Therefore, the database processes a significant quantity of personal data on each data subject and it concerns a large number of data subjects.

6.8 The processing on the ICB database occurs in the context of various ICB members feeding information into the centralised database and then accessing the database by making enquiries as required. This context creates a greater risk that the ICB might process inaccurate personal data because an error from any of the members could cause inaccuracy. The ICB could then share this inaccurate personal data with other members. The ICB relies on its members to submit accurate personal data. This context heightens the need for specific technical and organisational measures to protect the accuracy the personal data processed.

6.9 The purpose of the processing of personal data on the ICB database is to assist lenders in assessing credit applications from potential borrowers. The personal data also enables the ICB to produce credit reports and credit scores on data subjects. This, in turn, can lower the cost of credit, enable faster decisions, and assist with fraud prevention. However, the purpose of the processing is also linked to data subjects' interests in being able to access credit, and any inaccuracy is likely to adversely affect their rights and freedoms.

6.10 The risk to the rights and freedoms of natural persons posed by the processing on the ICB database is assessed objectively by reference to the likelihood of that risk and its severity. The processing creates the risk of ICB members submitting inaccurate personal data regarding data subjects' performance on credit agreements and of the ICB sharing that

inaccurate personal data with other ICB members. Recital 76 of the GDPR provides guidance as to how risk should be evaluated:

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

6.11 The risk assessment must consider, first, the likelihood of inaccurate personal data on data subject's performance on credit agreements being processed by the ICB and, second, the severity of that risk in respect of the rights and freedoms of the data subjects. These objective assessments are made by reference to the nature, scope, context and purposes of the processing as considered above.

6.12 I find that the likelihood of the risk of inaccurate personal data being processed on the ICB database is high. I make this finding in light of the high number of ICB members who are contractually obliged to provide updates to the database and how this results in 3.5 million monthly updates. [redacted]

6.13 I find that the severity of the risk to the rights and freedoms of natural persons flowing from inaccurate processing of personal data on the ICB database is also high. In particular, I make this finding in light of the sensitivity and purpose of the processing on the ICB database. Inaccuracies are likely to influence ICB members' decisions on the data subjects' access to credit. This is reflected in complaint C-18-10-11 received by the DPC, in which an ICB member questioned a data subject's mortgage application due to an error in a credit report resulting from the personal data breach. It is also reflected in the credit report referred to by the ICB member that made the ICB aware of the personal data breach, where ICB member noted the error appeared to be informing the credit score.

6.14 The ICB was obliged to have regard to this high risk when determining which measures to implement pursuant to Article 25(1). This high risk must also be considered against how the ICB relies on its members to submit accurate personal data. However, as outlined above, this does not relieve the ICB of its own obligation under Article 25(1) to implement appropriate measures designed to implement the accuracy principle. Despite the challenges faced by the ICB, it is clear that technical and organisational measures are available to reduce the risk of it processing inaccurate personal data.

6.15 The ICB implemented a technical measure to prevent payment profile updates to closed accounts by filtering such edits. By their very nature, payment profile updates to closed accounts are likely to be inaccurate because the accounts had previously closed. Therefore, such updates should ordinarily be avoided, save in exceptional circumstances, for example, to correct an error previously recorded on the account. The ICB unintentionally removed this measure on 28 June 2018 and re-implemented it on 30 August 2018. As a result, the ICB

failed to erase or rectify a large quantity of inaccurate personal data submitted by its members, and further processed some of this personal data by sharing it with other members. In the circumstances, I find that this technical measure is an appropriate measure that the ICB was obliged to implement pursuant to Article 25(1) of the GDPR. I accept that the ICB accidentally removed the filter. However, in doing so, it infringed Article 25(1) for just over 2 months in the circumstances.

6.16 The ICB used a change management process when implementing the code change. This change management process was set out in the *"ICB ISO Policy document"*[12]. In its submissions to the Case Officer on 15 August 2019, the ICB quoted the change management process that was in place at the time of the code change as follows:

> *"ICB operates change management processes in relation to the following resources; staff, business processes and all hardware and software related to the ICB Systems. The following process shall be followed for each change required:*
> *• the required change shall be discussed and documented with management;*
> *• if the change impacts on personal data stored on the ICB database, then a Privacy Impact Assessment (PIA) needs to be performed as per GDPR requirements. A template can be found here:*
> *http://icb-dc/GDPR/Shared%20Documents/Policies/PIA%20Template%20Draft.docx*
> *• a costing plan shall be produced and discussed with management to justify expenditure and obtain approval for the relevant expenditure;*
> *• a change management document shall be produced with agreed by all relevant parties;*
> *• Implementation plans, where required, are produced and agreed by all relevant parties to the change;*
> *• Changes to the operational systems (where possible) shall be made outside of prime service times and customers shall be given appropriate notice as defined in the Service Level Agreement. An exception to this shall be when an emergency change is required to rectify an issue that is causing disruption to the service. This emergency change must be authorised a senior manager and the change implemented as soon as can be arranged.*
> *Changes shall be executed with at least 2 members of the technical team and will include a back out plan to reverse the change as a contingency."*[13]

6.17 The ICB submitted that its change management process complied with the ISO27001 standard. The Organization for Stadardization (**"ISO"**) "*Code of practice for information security controls"*[14] provides guidance on change management as follows:

> ***"12.1.2 Change management***
> *Control*

[12] The ICB's response to the DPC's queries submitted by email on 15 August 2019.
[13] The ICB's response to the DPC's queries submitted by email on 15 August 2019 at page 4.
[14] ISO/IEC 27002:2013(E), Second edition, 2013-10-01.

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance
In particular, the following items should be considered:
a) identification and recording of significant changes;
b) planning and testing of changes;
c) assessment of the potential impacts, including information security impacts, of such changes;
d) formal approval procedure for proposed changes;
e) verification that information security requirements have been met;
f) communication of change details to all relevant persons;
g) fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;
h) provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (see 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Other information
Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see 14.2.2)."

6.18 The ISO's code of practice provides guidance for organisations implementing commonly accepted information security controls. It provides that the resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The code of practice provides that:

> *"This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required."*[15]

6.19 The ICB's change management process that was in place at the time of the code change did not make any provision for testing proposed coding changes, nor did it make any provision for a formal approval procedure for proposed coding changes. The process did not require any testing and it did not make provision for such testing to be documented if and when actually carried out. While the process did require changes to be discussed and documented with management, and it did require certain matters to be *"agreed by all relevant parties"*,

[15] At paragraph 0.4.

it did not provide a formal approval procedure. No provision of the change management process required proposed changes to be approved before being implemented and the process did not make any provision for how responsibility for approving proposed changes would be delegated. In this respect, having regard to the high risk outlined above, the ICB did not approach its obligation under Article 25(1) correctly.

6.20 A comprehensive change management process that provides for testing and a formal approval procedure for coding changes is essential to implementing the principle of accuracy in the circumstances. Such provisions would contribute to ensuring that all proposed changes are sufficiently scrutinised by the ICB prior to implementation by guiding such testing and by promoting accountability. This, in turn, would reduce the likelihood of coding errors that undermine measures designed to protect the accuracy of the personal data processed on the database, such as the filter on updates to completed accounts. In those circumstances, I find that implementing a comprehensive change management process, to include testing and a formal approval procedure for proposed coding changes, is an appropriate organisational measure that the ICB was obliged to implement pursuant to Article 25(1) of the GDPR.

6.21 I have also considered the guidance from the ISO, and while it does not expressly require a documented change management process, it does provide that formal management responsibilities and procedures for change management should be in place. It provides that consideration should be given to testing and a formal approval procedure for proposed changes. Furthermore, it acknowledges that resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The ICB operates a database with sensitive personal data concerning approximately 2.8 million data subjects. Changes to this database creates a high risk for rights and freedoms of natural persons. In those circumstances, a comprehensive change management process is appropriate to implement the principle of accuracy.

6.22 A technical measure to prevent payment profile updates to closed accounts and an organisational measure to implement a comprehensive documented change management process are measures that were readily available and mature solutions at the time of the personal data breach. I have had regard to the high risk caused by the processing on the database, the circumstances of the processing, the state of the art, and the cost of implementing these measures in finding that they were appropriate within the meaning of Article 25(1) of the GDPR. I consider that the measures could have been implemented by the ICB without entailing excessive cost or difficulties.

i. Findings

6.23 I find that the ICB infringed Article 25(1) of the GDPR both at the time of the determination of the means for processing and at the time of the processing itself on the ICB database, by failing to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect

the rights of data subjects. The appropriate technical and organisational measures that the ICB ought to have implemented include a technical measure to prevent payment profile updates to closed accounts during the period between 28 June 2018 and 30 August 2018; and a comprehensive documented change management process that makes express provision for, amongst other things, the testing of coding changes and a formal approval procedure for proposed coding changes.

7. Issue 2: Articles 5(2) and 24(1) of the GDPR

7.1 Article 5(2) of the GDPR provides:

> *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

7.2 Article 24 of the GDPR provides:

> *"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*
>
> *2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*
>
> *3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."*

7.3 Article 5(2) of the GDPR provides that controllers are responsible not only for complying with the data protection principles, but are also accountable for being able to demonstrate their compliance. Article 24(1) of the GDPR develops this accountability principle by requiring that controllers implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

7.4 This issue concerns whether the ICB complied with its obligation to demonstrate compliance. In considering this issue, it is necessary to first note that the ICB is required to carry out testing of proposed code changes to the ICB's database in order to ensure that its processing is performed in accordance with Article 25(1) of the GDPR. As outlined above, code changes to the ICB database create specific risks to the accuracy of the personal data processed on it. Having regard to the high risk for the rights and freedoms of natural persons, the state of

the art, and the cost of implementation, I find that testing of proposed changes is an appropriate measure, within the meaning of Article 25(1) of the GDPR. The ICB is obliged to implement this testing before making any changes to the code of its database. Therefore, this issue concerns whether the ICB demonstrated compliance with this obligation to undertake appropriate testing of proposed changes to its database.

7.5 The ICB submitted that it carried out testing of the proposed changes before implementing the code change. However, it did not maintain any records of the testing undertaken. Having regard to the high risk to the rights and freedoms of natural persons presented by the processing on the ICB database as outlined above, I find that the obligation to demonstrate compliance, pursuant to Articles 5(2) and 24(1) of the GDPR, required the ICB to maintain a documented record of the testing undertaken in respect of code change. In addition to demonstrating compliance as required by Articles 5(2) and 24(1), such records of testing are also useful for putting the data protection principles in Article 5(1) into practice. The testing undertaken by the ICB prior to the code change failed to identify that the proposed change would remove the filter that prevented updates to closed accounts. If the ICB had maintained records of the testing undertaken, it could analyse that testing with the benefit of hindsight, and potentially identify improvements to its future testing. This, in turn, would reduce the risk of similar code errors occurring in the future. Furthermore, a record of the testing undertaken could assist the ICB in identifying why they only became aware of the personal data breach when an ICB member notified them of an error regarding a customer credit card record over 8 weeks after the code change.

7.6 The ICB submitted that *"the code change was tested per ISO requirements by ICB technical staff"*[16]. I have had regard to the ISO standards as relied upon by the ICB In the context of demonstrating compliance with its testing obligations. The ISO's Code of practice for information security controls provides that changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems[17]. The Code also provides that testing of security functionality should be carried out during development[18] and that acceptance testing programs should be established for new information systems, upgrades and new versions[19]. The code also provides that when changes are made to information processing facilities and systems that affect information security, an audit log containing all relevant information should be retained[20]. The ISO's *"Information security risk management"*[21] standard provides methods for assessing technical vulnerabilities in the context of risk management. These methods include Security Testing and Evaluation and Code Review, amongst others[22].

[16] ICB submissions dated 15 August 2019.
[17] Control 12.1.4 at page 41.
[18] Control 14.2.8 at page 61.
[19] Control 14.2.9 at page 61.
[20] Ibid at page 39.
[21] ISO/IEC 27005:2018(E), Third edition, July 2018.
[22] Ibid at page 44.

7.7 The ISO standards relied on by the ICB provides guidance to organisations for approaching the obligation to test changes to information security management systems. Complying with the standards does not result in a documented record of testing undertaken by the ICB. The ICB's statement that the code change was tested per ISO requirements does not demonstrate compliance with its obligation to test the code because it does not record the steps undertaken by the ICB in applying this guidance and in implementing appropriate testing. In the absence of a documented record of the testing actually undertaken, the ICB has failed to demonstrate compliance with its obligation to undertake appropriate testing.

7.8 The ICB submitted a blank Data Protection Impact Assessment template during the Inquiry. This DPIA contains no documented record of the testing that the ICB decided to apply. The ICB also submitted a change control form, titled *"Irish Credit Bureau Change Request – PP Update"*, dated 28 June 2018. This change control form included an *"Impact Assessment"* that stated that the risk assessment was *"Medium".* I have had regard to these documents in the context of the ICB's obligation to maintain a documented record of the testing. The documents contain no analysis of the nature of the risk and fail to identify any measures to mitigate any existing risk. [redacted] The ICB's submissions outlined that the technical staff implementing the change did not test for the filter that blocked updates to closed accounts, which the ICB implemented 20 years previously, as they were unaware of the nature of the updates received from some member systems. Had a risk analysis been appropriately implemented, the risk of the filter being removed would have been identified. The risk analysis would also have identified appropriate testing for the filter. Therefore, a properly documented risk analysis would have assisted the ICB not only in identifying appropriate testing, but also in demonstrating compliance with its obligation to carry out such testing. However, the blank Data Protection Impact Assessment and the change control form submitted by the ICB did not identify the nature of the risks, and did not demonstrate the ICB's compliance with its obligation to undertake appropriate testing of proposed changes to its database.

7.9 The ICB has failed to maintain a documented record of the testing undertaken in respect of the code change and, accordingly, I have not been able to assess the adequacy of the testing undertaken. In those circumstances, I find that the ICB has infringed Articles 5(2) and 25(1) of the GDPR by failing to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database.

i. Finding

7.10 I find that the ICB infringed Articles 5(2) and 24(1) of the GDPR by failing to demonstrate compliance with its obligation, pursuant to Article 25(1) of the GDPR, to undertake appropriate testing of proposed changes to its database.

8. Issue 3: Article 26(1) of the GDPR

8.1 Article 26(1) of the GDPR provides:

> *"Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects."*

8.2 The obligation in Article 26(1) to implement an arrangement applies only to joint controllers. Joint controllership arises where two or more entities jointly determine the purposes and means of a particular processing operation. The processing operations under consideration in this Decision concern the operation of the ICB database. In order for joint controllership to exist, the ICB must jointly determine both the purposes and means of the processing with another entity; it is not sufficient for joint determination to occur in relation to either one of the purposes or the means alone.

8.3 In *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Manni*[23] the Court of Justice of the European Union considered the processing of personal data on a companies register maintained by the Lecce Chamber of Commerce. The register identified the director of an insolvent company. In relation to the issue of controllership, the Court held that:

> *"by transcribing and keeping that information in the register and communicating it, where appropriate, on request to third parties, the authority responsible for maintaining that register carries out 'processing of personal data' for which it is the 'controller', within the meaning of the definitions set out Article 2(b) and (d) of Directive 95/46."*[24]

8.4 The purposes of the processing of personal data on the ICB database is set out in the agreement entered into between the ICB and its members. The ICB submitted a template of this agreement to the Case Officer. That agreement provides that *"…all data and information received by the Member from the ICB may only be used for credit assessment and account maintenance purposes."*[25] I am satisfied that the ICB processes personal data on its database in order to make the personal data available to relevant lenders for credit assessment and account maintenance purposes. The concept of controller is determined by a factual rather than a formal analysis. This means that it is necessary to look past the written agreement

[23] Case C-398/15, Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, judgment of 9 March 2017 (ECLI:EU:C:2017:197).
[24] At paragraph 35.
[25] At clause 2.6.

and to look at which entities actually exercise determinative influence over why the processing is taking place and for which purpose. I am satisfied that both the ICB and its members jointly determine the purposes of the processing on the database. The members of the ICB agree to register credit agreements so that the ICB can process this personal data for the benefit of the members' credit assessment and account maintenance purposes. These are common purposes shared by the ICB and its members and I am satisfied that both parties factually determine these purposes for the submission, storage, and retrieval of the information on the database when entering the agreement.

8.5 Many of the essential means of the processing on the ICB database were set out in the *"ICB Members' Technical Manual July 2015"* during the time under consideration in this Decision. The technical manual determined the duration of processing on the database by providing that *"Loan Data is retained on the ICB database for 5 years from the time the agreement is closed"*[26]. The technical manual determined how the database is updated and provided detailed specifications for how members must send updates to the ICB[27]. The manual also provided detailed specifications for how members can request information from the system and how the replies are sent[28]. The technical manual also determined the extent of the types of personal data processed on the database. For example, paragraph 4.3.1 specifies the mandatory personal data that members must submit when registering an account holder. This includes the account holder's name and address, their gender, occupation, date of birth, and telephone number. The ICB furnished the Technical Manual to its members. I am satisfied that the ICB has alone determined the means of processing specified in the Technical Manual.

8.6 The ICB also determined who had access to the database. This is one of the essential means of the processing on the database. As outlined above, the ICB members are contractually obliged to register credit agreements with the ICB and are entitled to access to the ICB's full range of credit reference services. The ICB determines which entities may become ICB members and therefore the ICB determines the categories of recipients of the personal data. The ICB also determined the nature of the processing on the database by devising its own system of generating credit scores. The ICB alone determined how these scores are calculated.

8.7 I find that the ICB determines the essential means of the processing of personal data on the ICB database and that there is no evidence that any other entity has jointly determined those means. There is no evidence that the ICB members, or any entity other than the ICB, exercise determinative influence over the means of the processing on the ICB database. Therefore, I in circumstances where the ICB determines the purposes and means of the processing on the database, I find that it alone is the controller of the database. Therefore, the transmission of personal data from ICB members to the ICB, and vice versa, constitute disclosures of personal data between two controllers.

[26] At paragraph 7.3.
[27] Part 4 of the Technical Manual titled "New Business and Updates".
[28] Part 4 of the Technical Manual titled "Enquiry Subsystem".

ii. Finding

8.8 I find that the ICB did not infringe Article 26(1) of the GDPR. The ICB members are not joint controllers in respect of the ICB database and therefore there was no obligation on the ICB or the members to determine their respective responsibilities for compliance with the GDPR by means of an arrangement.

9. Decision on Corrective Powers

9.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that the ICB has infringed Articles 25(1), 5(2), and 24(1) of the GDPR. Under Section 111(2) of the 2018 Act, I must now, make a decision as to whether corrective powers should be exercised in respect of the ICB and, if so, the corrective powers to be exercised. The remaining question for determination in this Decision is whether or not those findings merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

9.2 Recital 129, 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..."*

9.3 In the circumstances of the within inquiry and the findings of infringements, 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. Having carefully considered the infringements identified in this Decision, 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 the ICB in respect of its infringements of Articles 25(1), 5(2), and 24(1) of the GDPR; and
b) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of the ICB's infringement of Article 25(1) of the GDPR.

9.4 The Draft Decision provisionally proposed to order the ICB to bring its processing operations regarding its database into compliance with Article 25(1) of the GDPR in accordance with Article 58(2)(d) of the GDPR. That provisional order would have required the ICB to implement a formal approval procedure for proposed code changes on the ICB database. In making that provisional order, the Draft Decision had due regard to the measures implemented by the ICB since the personal data breach, including its updated change management process as set out in the *"ICB ISO Policy document"*, dated 15 December 2020.

That updated change management process did not include a formal approval procedure: it did not require proposed changes to be approved before being implemented and it did not make any provision for how responsibility for approving proposed changes should be delegated. In this context, the Draft Decision proposed to order the ICB to implement a formal approval procedure for proposed coding changes on the ICB database.

9.5 The ICB's submissions on the Draft Decision appended the *"Irish Credit Bureau Change Management Policy"*, dated 17 February 2021. The ICB created this policy during the course of the Inquiry. It is applicable to all systemic change, organisational change, and change in projects in the ICB, including code changes. The policy introduces a formal approval requirement during the five stages outlined throughout the ICB's change process and sets out responsibility for approving change requests. It also provides that the CEO must approve high risk changes, and this category expressly includes changes where personal data is affected. The ICB's accompanying change control forms also include a specific section requiring approval. The ICB submitted that the proposed order in the Draft Decision is no longer necessary in light of the ICB's updated formal approval procedure. I accept this submission. Since the personal data breach, I am satisfied that the ICB has implemented a formal approval procedure that requires proposed changes to be approved before being implemented and that makes provision for how responsibility for approving proposed changes should be delegated. This procedure, if properly implemented by the ICB, would ensure that proposed coding changes are analysed, and that responsibility is appropriately delegated, before changes are made that could affect the accuracy of the personal data processed on the ICB's database. In those circumstances, it is not appropriate or necessary for this Decision to make an order pursuant to Article 58(2)(d) of the GDPR.

A. Reprimand

9.6 I issue the ICB with a reprimand in respect of its infringements of Articles 25(1), 5(2), and 24(1) 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."* I consider that a reprimand is appropriate, necessary and proportionate in view of ensuring compliance with the infringed Articles, as the reprimand will act to formally recognise the serious nature of all of the infringements. Further, the reprimand emphasises the requirement for ICB to take all relevant steps to ensure future compliance with the infringed Articles. It is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. Furthermore, each measure that I impose 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 a reprimand in addition to the administrative fine detailed below in order to give full effect to the obligations in Articles 25(1), 5(2), and 24(1) and to formally recognise the seriousness of the infringements found in this Decision.

B. Administrative Fine

9.7 I find that the ICB's infringement of Article 25(1) of the GDPR warrants the imposition of an administrative fine pursuant to Article 58(2)(i) GDPR in addition to the reprimand. The reason for that decision and the method for calculating that fine are set out below.

i. Whether Each Infringement Warrants an Administrative Fine

9.8 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 Data Protection Act, 2018, which permits the DPC to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2). 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 an administrative fine and the amount of any such fine, I must give due regard to the criteria set out in Article 83(2) GDPR, which provide that:

> *"Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*

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

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

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

9.9 The decision as to whether to impose an administrative fine (and if so, the amount of the fine) is a cumulative decision which is taken having had regard to of 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 the ICB's infringements of Article 25(1), and Articles 5(2) & 24(1) respectively:

a) <u>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;</u>

9.10 The nature of the ICB's infringement of Article 25(1) comprises a failure to implement appropriate technical and organisational measures designed to implement the principle of accuracy in its database. Specifically, the infringement of this Article concerned the ICB's failure to utilise a technical measure to prevent payment profile updates to closed accounts and a failure to implement a comprehensive documented change management process. The objective of Article 25(1) is to ensure that controllers implement appropriate measures designed to implement the data-protection principles, including the principle of accuracy. In assessing the nature of the infringement of Article 25(1), I have had regard to the scope and purpose of the processing on the ICB database. The database contains information relating to approximately 2.8 million data subjects and the ICB submitted that this figure does not vary significantly from year to year[29]. The database records the performance of credit agreements concerning ICB members with the purpose of assisting those members in assessing credit applications from potential borrowers. Therefore, accuracy in the database is essential to ensuring fairness in respect of data subjects' applications for credit. It is paramount for this purpose that the ICB implements appropriate technical and organisational measures to ensure the accuracy of the personal data processed on the database. The ICB's infringement of Article 25(1) undermined the accuracy of 15,120 closed loan records. In those circumstances, I find that the nature of the ICB's infringement of Article 25(1) is serious.

9.11 The nature of the ICB's infringement of Article 5(2) and 24(1) of the GDPR comprises a failure to demonstrate compliance with its obligation, pursuant to Article 25(1) of the GDPR, to undertake appropriate testing of proposed changes to its database. Specifically, this infringement concerns the ICB's failure to maintain a documented record of the testing

[29] ICB submissions on the Draft Decision, dated 23 February 2021, at page 6.

undertaken in respect of coding changes to the database. The objective of Articles 5(2) and 24(1) of the GDPR include not only ensuring compliance with the data protection principles, but also ensuring that controllers are able to demonstrate that compliance to supervisory authorities. I consider that these articles are crucial to the oversight and enforcement actions of supervisory authorities, such as the DPC. Non-compliance with these articles may prevent or hinder a supervisory authority in its enforcement action designed to protect the rights and freedoms of data subjects. In the particular circumstances, the ICB's failure to maintain a documented record of the testing undertaken has prevented the DPC from analysing the adequacy of that testing. In those circumstances, I find that the nature of the ICB's infringement of Articles 5(2) and 24(1) is also serious.

9.12 In assessing the gravity of the ICB's infringement of Article 25(1), I have had regard to the number of data subjects affected and the level of damage suffered by them. The ICB's failure to implement a technical measure to prevent payment profile updates to closed accounts, and its failure to implement a comprehensive documented change management process, directly contributed to the personal data breach. This breach resulted in the ICB database recording an incorrect payment history of 15,120 accounts. This could have influenced the credit ratings of 15,120 data subjects had all of those records been accessed. However, the ICB disclosed 1,062 of the inaccurate accounts to ICB members and directly to data subjects before it fixed the issue. The principle of accuracy requires that any personal data stored on the ICB database must be accurate irrespective of whether the ICB views or shares that personal data. Therefore, in considering the number of data subjects affected by the ICB's infringement, it is appropriate to have regard to the 15,120 inaccurate accounts. However, in respect of the level of damage suffered by the data subjects, I accept that the personal data breach did not affect the credit ratings of most of the affected data subjects because the ICB creates credit ratings only when requested by ICB members. Therefore, the level of damage suffered by most of the 15,120 data subjects was minimal. However, the disclosure 1,062 of the inaccurate accounts, nonetheless, reflects a highly significant number of data subjects.

9.13 Turning to the level of damage suffered by the data subjects in respect of the 1,062 inaccurate disclosed accounts, the ICB submitted that the inaccuracies caused a minimal impact on data subjects and that the gravity of this infringement should be assessed as moderate to minor. In this regard, the ICB submitted that the only change on the closed loan account for the vast majority of those accounts was the date the account closed. All the account records that were disclosed to ICB members were limited to this inaccuracy alone. The ICB submitted that the potential impact of this inaccuracy was minimal and that the disclosure of this inaccurate data to ICB Members was unlikely to cause ICB members to refuse credit. The ICB also outlined how it did not receive any complaints from the 118 data subjects who obtained an incorrect credit report. The ICB did not notify the remainder of the data subjects in respect of the 1,062 inaccurate disclosed accounts. However, it did ask its members to confirm to the ICB if it had been necessary for the members to contact any data subjects arising from those members' reviews of their lending decisions. The ICB informed the DPC that it *"has not been advised by any member that any of this population of data subjects had an application for credit declined because of the incorrect closure date*

on a closed account."[30] However, the ICB also acknowledged in its submissions that an ICB member's internal processes and practices will also play a significant role in their lending decisions and rating the credit worthiness of an individual and that the same data provided from ICB can lead to different lending decisions being taken by different lenders[31].

9.14 I do not accept the ICB's submission that the inaccuracies caused a minimal impact on the data subjects in respect of the 1,062 inaccurate disclosed accounts in the circumstances. The ICB discloses personal data to its members in order to assist them in making decisions on applications for credit. This personal data includes the date on which accounts closed. The inclusion of this personal data by the ICB suggests that it is relevant to the ICB's purpose of processing that data i.e. assisting ICB members' decisions on credit. This is consistent with the ICB's own letters sent to data subjects on 21 September 2018 in which it stated that *"If you applied for a loan with an ICB member during this period it could have affected that member's decision on that loan application."* Where inaccurate personal data are disclosed to an ICB member for the purpose of assisting that entity in assessing applications for credit, this significantly deprives data subjects of control over their personal data.

9.15 A complaint received by the DPC concerning the personal data breach further illustrates how inaccurate information regarding the date on which accounts closed can adversely affect data subjects. The DPC received complaint C-18-10-11 in which a data subject stated, *"I have not been granted a mortgage due to this gross error on the part of ICB"*. The complainant's credit card finalisation date had been inaccurately altered from February 2015 to February 2018. This inaccurate personal data was shared with an ICB member. The complainant had given the true date in a mortgage application, but the inaccuracy on the credit report caused the relevant bank to question that application. The complainant was ultimately granted a mortgage from another bank, which happened to be the same bank that submitted the inaccurate personal data to the ICB (and therefore was in a position to verify the inaccuracy itself). The complaint to the DPC was resolved amicably. While the original bank did not reject the application and the data subject instead proceeded with another bank, this complaint illustrates the relevance of the date on which accounts closed to ICB members' decisions on applications for credit. Such inaccurate information could also cause ICB members to question the accuracy of truthful information submitted by data subjects in applications for credit.

9.16 Article 83(2)(a) requires that I must take into account the level of damage suffered by data subjects in assessing the criteria under that sub article. I consider that the level of damage suffered by data subjects is relevant in assessing the gravity of the ICB's infringement of Article 25(1). Recital 75 of the GDPR describes the "damage" that can result where processing does not accord with the requirements of the GDPR:

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise*

[30] ICB submissions on the Draft Decision, dated 23 February 2021, at page 10.
[31] Ibid.

to…any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data…"

9.17 The personal data breach prevented the data subjects in respect of the 1,062 inaccurate disclosed accounts from exercising control over their personal data. In order for data subjects to exercise control over their personal data, they must able to predict with sufficient certainty which personal data about them is being processed. The personal data breach inaccurately amended the dates of the closed accounts, for a period that lasted up to 9 weeks, without notifying the data subjects. While the data subjects had the right to access this personal data during that period, it is significant that all of the inaccurate personal data related to closed accounts. Those data subjects may have justifiably assumed that their personal data concerning those closed accounts would not be subject to amendment after the account closed. Hence, those data subjects may have been less likely to seek to verify the accuracy of their personal data concerning accounts that had closed up to five years previously. The inaccuracy is compounded by the purpose for which the inaccurate personal data was shared with ICB members. The fact that ICB members were accessing this personal data suggests that they may have actively been considering applications for credit from the data subjects. Therefore, not only was there a loss of control, but there was also a risk of economic disadvantage arising from the ICB's disclosure of the inaccurate data. For instance, in complaint C-18-10-11, the inaccuracy caused, at a minimum, a delay in the data subject's mortgage application and resulted in the data subject proceeding with another bank. Therefore, the personal data breach caused economic disadvantage that is significant in that case. Furthermore, the ICB member who notified the ICB of the personal data breach on 27 August 2018 also identified that the issue was influencing the data subject's credit score. While it is not possible to detail the precise damage suffered by each of the data subjects in respect of the 1,062 inaccurate disclosed accounts, the potential for damage to those data subjects is a relevant factor to take into consideration in my analysis as to whether a fine should be imposed under Article 83 and, if so, the amount of that fine. I find that the loss of control, and the potential for economic disadvantage, resulted in the data subjects suffering a high level of cumulative damage.

9.18 I find that the gravity of the ICB's infringement of Article 25(1) was severe. In making this finding, I have had regard to the fact that the personal data breach affected the accounts of 15,120 data subjects. However, I have balanced this with how the level of damage suffered by most of those data subjects was minimal in circumstances where the ICB fixed the inaccurate data without disclosing all but 1,062 of those inaccurate accounts. Nonetheless, this smaller number is still a highly significant number of inaccurate accounts. This resulted in a high level of cumulative damage across the high number of data subjects. The data subjects were prevented from exercising control over their data and there was significant potential for economic disadvantage from the breach in circumstances where the ICB members used the inaccurate personal data in considering applications for credit from those data subjects.

9.19 In assessing the gravity of the ICB's infringement of Articles 5(2) and 24(1), I have had regard to the manner in which the infringement prevented the DPC from analysing the adequacy of the testing undertaken by the ICB. However, the ICB maintains that its testing was sufficient. The finding of an infringement of Articles 5(2) and 24(1) relates to the ICB's failure to maintain a documented record of the testing undertaken and this decision does not make any finding in relation to the adequacy of the testing. Therefore, in assessing the gravity of the infringement, it is not appropriate to have regard to whether the level of testing contributed to the personal data breach. In those circumstances, I find that the gravity of the ICB's infringement of Articles 5(2) and 24(1) was moderate.

9.20 Regarding the duration of the infringement of Article 25(1), the ICB removed the measure that filtered payment profile updates to closed accounts on 28 June 2018 and re-implemented it on 30 August 2018. Therefore, the duration of this element of the infringement was 2 months and 2 days. Prior to, and during that period, the ICB also failed to implement a comprehensive documented change management process. Therefore, for the purposes of this Decision, the duration of this element of the infringement must be assessed as commencing on 25 May 2018, at the enactment of the GDPR. As outlined above, the ICB implemented a comprehensive documented change management process during the course of the Inquiry and I am satisfied that this element of the infringement was addressed when the ICB implemented its *"Irish Credit Bureau Change Management Policy"*, dated 17 February 2021. Therefore, the duration of this element of the infringement was 2 years and 8 months in length. However, the element of this infringement concerning the technical measure was limited to 2 months and 2 days.

9.21 Regarding the duration of the infringement of Articles 5(2) and 24(1), the ICB submitted that it carried out testing of the proposed changes before implementing the code change. However, these infringements relate to its failure to maintain a documented record of that testing rather than the adequacy of the testing. The *"Irish Credit Bureau Change Request – PP Update"* provides that the change request date was 9 March 2018. The code change was then implemented on 28 June 2018. Therefore, it is clear that the ICB's failure to maintain a documented record of its testing in relation to this code change occurred between 9 March 2018 and 28 June 2018. In those circumstances, the infringement of Articles 5(2) and 24(1) commenced at the enactment of the GDPR on 25 May 2018 and ended on 28 June 2018. Therefore, the duration of the infringements was 1 month and 3 days.

b) <u>the intentional or negligent character of the infringement;</u>

9.22 The ICB implemented the code change with the intention of improving the accuracy of the database by making provision for the infrequent cases where a customer of an ICB member subsequently pays a contribution towards an account that was written-off, or that had goods repossessed or surrendered.

9.23 The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 provide that:

"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."[32]

9.24 I am satisfied that the ICB's infringements of Articles 25(1), 5(2), and 24(1) were not intentional on the part of the ICB. The removal of the filter to prevent payment profile updates to closed accounts was unintentional and the intent of the ICB was to improve, rather than damage, the accuracy of the database. Therefore, there was no knowledge or wilfulness on the part of the ICB in this respect. Furthermore, there is no evidence of knowledge or wilfulness on the part of the ICB in respect of its failure to implement a comprehensive documented change management process, nor its failure to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database. Therefore, I find that the ICB's infringements of Articles 25(1), 5(2), and 24(1) were not intentional.

9.25 I find that the ICB's infringements of Articles 25(1), 5(2), and 24(1) were negligent in character within the meaning of Article 83(2)(b). I find that this is an aggravating factor in the context of determining whether to impose an administrative fine and the amount of that fine, if applicable, in the circumstances. I accept the ICB's submission that the presence of negligence does not automatically lean towards the imposition of an administrative fine. However, in the particular circumstances, the ICB's negligence is aggravating, and cannot be considered neutral or mitigating. Firstly, the processing of personal data is at the core of the ICB's business activities. It operates a complex database that processes a significant amount of personal data, and works with financial institutions in obtaining and sharing this personal data. In those circumstances, it ought to have been aware of the precise extent of its obligation to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner. The ICB also ought to have been aware of its obligation to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database. Secondly, its failure to implement a comprehensive documented change management process was not the result of the ICB misinterpreting its obligations, nor was it the result of the ICB seeking to innovate the manner in which it complies. The ICB did not seek to implement alternative measures instead of providing for testing and a formal approval procedure in the change management process. This illustrates that the ICB did not did not give sufficient attention or resources to implementing the principle of accuracy. In all the circumstances, I find that the presence of negligence is aggravating. While this is an aggravating factor, I have had regard to the fact that the infringement was not intentional or wilful in attaching weight to this aggravating factor and in the context of whether to impose an administrative fine and, if so, the amount of that fine.

[32] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' at page 11.

c) <u>Any action taken by the controller or processor to mitigate the damage suffered by data subjects;</u>

9.26 I find that the ICB took significant action to mitigate the damage suffered by data subjects. The ICB became aware of a potential issue regarding its database on 27 August 2018, it promptly investigated the issue, and determined on 29 August 2018 that the code change caused the error by removing the filters on the ICB database. The ICB fixed the validation rules on 31 August 2018 and corrected the affected data on that date. Therefore, I am satisfied that the ICB acted expeditiously in addressing the underlying technical issue and in correcting the inaccurate data.

9.27 On 31 August 2018, the ICB notified 3 ICB members, whose updates accounted for 98% of incorrect account records, of the personal data breach. The ICB notified the remaining 20 of its members, whose updates accounted for 2% of incorrect account records, of the personal data breach by 5 September 2018. It also notified the 118 data subjects, who had obtained an incorrect credit history check directly from the ICB, of the personal data breach. By 21 September 2018, the ICB wrote to the ICB members who received inaccurate data in response to a credit history check and advised those members that they should review any credit decision made based on that affected data. I consider that these actions helped to mitigate the damage suffered by those data subjects. The ICB did not notify the data subjects whose inaccurate accounts were shared with ICB members. However, it did ask its members to contact any data subjects whose credit application may have been adversely affected by the inaccurate data.

9.28 The ICB notified the DPC of the personal data breach without undue delay pursuant to its obligation under Article 33(1) of the GDPR. This allowed the DPC to assess the circumstances of the personal 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. However, for an action carried out by a controller to be considered a mitigating factor, it must be a voluntary remedial action, whereby the controller takes *"responsibility to correct or limit the impact of their actions"*[33]. An action, taken by a controller where it is mandated to do so on foot of a statutory obligation is not a mitigating factor for these purposes. Therefore, I do not consider the ICB's notification of the personal data breach to the DPC mitigating.

d) <u>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;</u>

9.29 As outlined above, the ICB infringed Article 25 of the GDPR by failing to implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. I consider that the ICB holds a high degree of responsibility for this failure and that

[33] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, page 13.

the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringement of Article 25 against the ICB, this factor cannot be considered aggravating in respect of the infringements.

e) <u>any relevant previous infringements by the controller or processor;</u>

9.30 There are no relevant previous infringements by the ICB. The ICB submitted that it has a positive track record for over 30 years in processing the sensitive personal data held on its database. I accept the ICB's submission that this is an important factor that I must consider in relation to the appropriateness of imposing an administrative. I also accept that this is a mitigating factor in calculating any fine in the event that it is necessary to impose an administrative fine.

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

9.31 The ICB cooperated fully with the DPC to remedy the infringements and to mitigate their possible adverse effects. It initiated a range of remediation steps in response to the personal data breach. Regarding its infringement of Articles 5(2) and 24(1) of the GDPR, the ICB implemented new measures to address its requirement to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database. It's revised Operations Security Policy makes express provision for testing in relation to ICB system software, requiring a test plan, test case/results, and an implementation plan for all relevant changes. The ICB also implemented the ICB Testing Policy and Procedures, the ICB Test Plan Template, and the ICB Test Case Template, which further set out the testing procedures implemented by the ICB. The Test Case Template will provide a detailed record of the testing steps undertaken by ICB in relation to future changes. The ICB's process now requires that the Test Plan Template and Test Case Template must be completed for all testing conducted by the ICB.

9.32 The ICB also undertook an extensive review and amendment of its technical and organisational measures to ensure compliance with Article 25 of the GDPR. On discovery of the technical error, ICB immediately investigated the error and took immediate remediation action. It undertook a remediation governance review aimed at improving its existing framework. The ICB's technical working group met almost weekly to review progress in strengthening ICB's technical and organisational measures. The ICB created new policies and processes in relation to change control and testing, and updated its existing policies and processes. I have had regard to the suite of documentation submitted by the ICB with its submissions on the Draft Decision, and those submitted throughout the Inquiry, as detailed in the appendix to this Decision. These documents illustrate the gradual measures implemented by the ICB in response to the personal data breach, the Inquiry, and finally the Draft Decision. As outlined above, the measures implemented include a comprehensive change management process that provides for testing and a formal approval procedure for, amongst other things, coding changes. The process requires proposed changes to be approved before being implemented and delegates responsibility for approving proposed changes. I find that the ICB has shown a high degree of cooperation with the DPC and has

taken comprehensive steps to remedy the infringement of Article 25(1) and to mitigate its adverse effects.

g) <u>the categories of personal data affected by the infringement;</u>

9.33 The categories of personal data affected by the infringements of Articles 25(1), 5(2), and 24(1) include sensitive personal data. However, the personal data does not include special category personal data or data relating to criminal convictions as provided for in Articles 9 and 10 of the GDPR respectively. In its submissions on the Draft Decision, the ICB acknowledged that it processes sensitive personal data, but submitted that the reference to categories in Article 83(2)(g) means that the supervisory authority should consider if the data controller was processing special category personal data (Article 9 of the GDPR) or data relating to criminal convictions (Article 10).

9.34 The Administrative Fines Guidelines provide the following key questions for supervisory authorities when consider the categories of personal data pursuant to Article 83(2)(g):

> *"Does the infringement concern processing of special categories of data set out in articles 9 or 10 of the Regulation?*
> *Is the data directly identifiable/ indirectly identifiable?*
> *Does the processing involve data whose dissemination would cause immediate damage/distress to the individual (which falls outside the category of article 9 or 10)?*
> *Is the data directly available without technical protections, or is it encrypted?"*[34]

9.35 It is clear that the presence of special category personal data and data relating to criminal convictions are important matters to consider when applying Article 83(2)(g). However, the third question above acknowledges that other sensitive personal data are relevant when applying Article 83(2)(g). This is consistent with the purpose of Article 83(2)(g), which is to ensure that each supervisory authority gives due regard to the categories of personal data affected when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine. In this regard, the purpose of Articles 9 and 10 of the GDPR is to provide special protection to certain types of personal data by setting out specific rules for the processing of those types of personal data. It is not the purpose of articles 9 and 10 to limit the entire GDPR generally to certain specific tiers of personal data whenever it is necessary to consider the categories of personal data being processed. For instance, in the context of transfers, Article 49(5) refers to *"specific categories of personal data"*, thus, acknowledging that there are a range of distinct categories of personal data beyond a simple tiered system of categorisation. Therefore, the position that the effect of Articles 9 and 10 is to limit the GDPR's general consideration of categories of personal data to considering whether the personal data is special category, data relating to criminal convictions, or whether it falls into a third catch-all category, is not sustainable. In the context of applying Article 83(2)(g) (as distinct from applying Articles 9 or 10), it is necessary to consider the precise categories of personal data involved and the sensitivity of those categories.

[34] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 14.

9.36 While data subjects' performance on credit agreements is not special category personal data within the meaning of Article 9 of the GDPR, nor does it concern processing of personal data relating to criminal convictions and offences or related security measures within the meaning of Article 10 of the GDPR, this category of personal data is, nonetheless, highly sensitive in the circumstances. As outlined above, any mishandling of this personal data, due to inaccuracy, unauthorised disclosure, or otherwise, may seriously infringe the rights and freedoms of data subjects. Therefore, I find that this category of personal data is highly sensitive. In those circumstances, this is an aggravating factor for the purpose of deciding whether to impose and administrative fine, and if so, the amount of that fine.

h) <u>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;</u>

9.37 The Inquiry was conducted to examine whether or not the ICB has discharged its obligations in connection with the subject matter of the personal data breach and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the ICB in that context. Hence, the ICB's notification of the personal data breach indirectly contributed to the infringements becoming known to the DPC. The ICB submitted that the Draft Decision's proposal to treat the ICB's notification of *"the infringement"* to the DPC as a neutral factor fails to properly assess the criteria set out in Article 83(2)(h). It is important to note that notifying a personal data breach will not always necessarily equate to notifying an infringement of the GDPR because not all personal data breaches will necessarily indicate an underlying infringement of a provision of the GDPR. Nonetheless, in this case, the notification of the personal data breach indirectly contributed to the infringements becoming known to the DPC.

9.38 The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> *"The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor."*[35]

9.39 The ICB's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 25(1), 5(2), and 24(1). Therefore, this factor is not mitigating. However, as set out above, I have had regard to the circumstances of this individual case and the ICB's response to the personal data breach in considering Article 83(2)(c) and (f) above. Specifically, this includes the action taken by the ICB to mitigate the damage suffered by data subjects and the cooperation it gave in remedying the infringement and mitigating the possible adverse effects of the infringement. However, the ICB's notification to the DPC itself is not mitigating because it

[35] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 15.

was obliged to notify under Article 33(1) in circumstances where the personal data breach resulted in a risk to the rights and freedoms of the data subjects.

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;

9.40 Corrective powers have not previously been ordered against the ICB with regard to the subject-matter of this Decision.

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

9.41 The ICB achieved ISO27001 certification in October 2012 and has maintained its certification with 6 monthly audits by Certification Europe. There are currently no fully approved national certification schemes or mechanisms in line with Article 42 of the GDPR. This factor in Article 83(2)(j) is limited to approved codes of conduct or certification mechanisms. Therefore, this factor cannot currently be considered mitigating nor aggravating in the circumstances.

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.

9.42 I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

9.43 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. The Administrative Fines Guidelines provide that:

> *"The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both)."*[36]

9.44 The Draft Decision provisionally proposed to impose an administrative fine in respect of the ICB's infringement of Article 25(1) of the GDPR. That Draft Decision made the provisional finding that the administrative fine was necessary in respect of that infringement in order to effectively pursue the objective of re-establishing compliance with Article 25(1) and in providing an effective, proportionate and dissuasive response in the particular circumstances of this case. The ICB submitted that its infringement of Article 25(1) of the GDPR does not warrant the imposition of an administrative fine. In making this submission,

[36] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

the ICB highlighted how the Draft Decision's objective in proposing an administrative fine was to re-establish compliance. The ICB submitted that it has undertaken extensive remediation measures, both during the DPC's Inquiry and following the Draft Decision. In those circumstances, the ICB submitted that would not be *"effective, proportional, and dissuasive with a view to re-establishing compliance as ICB is now in full compliance with Article 25 of the GDPR."*[37] The ICB submitted that the proposed reprimand alone was proportionate in light of the remediation steps.

9.45 I have had regard to the extensive remediation measures implemented by the ICB since the personal data breach. These measures reflect significant efforts from the ICB to re-establish compliance with Article 25(1). Therefore, in deciding whether to impose an administrative fine, I must consider the suitability of a fine for the purpose of re-establishing compliance in light of those measures. I find that an administrative fine is necessary in respect of the ICB's infringement of Article 25(1), despite the remediation measures, in order to effectively pursue the objective of re-establishing compliance with Article 25(1) and in providing an effective, proportionate and dissuasive response in the particular circumstances of this case

9.46 Despite the remediation undertaken by the ICB, a fine is necessary in respect of the objective of re-establishing compliance. Article 25(1) places a continuous obligation on controllers to implement appropriate technical and organisational measures designed to implement the principle of accuracy. The obligation in article 25(1) requires the ICB to proactively, at both at the time of the determination of the means for processing and at the time of the processing itself, assess the risk, the state of the art, the cost of implementation and the nature, scope, context and purposes of its processing. An administrative fine is effective and proportionate in dissuading non-compliance because such non-compliance could flow from a failure on the part of the ICB to continually assess the appropriateness of its measures at the time of the processing itself. It is not sufficient for the ICB to simply respond to personal data breaches if, and when, they occur. The ICB must continually have regard to future changes in the risk, the state of the art and it's processing in ensuring that it has implemented appropriate measures designed to implement all of the data-protection principles. This is essential for compliance with Article 25(1). Ensuring compliance with this obligation is particularly important in light of the nature of the ICB's database. The 15,120 inaccurate closed loan records represented just 0.43% of the closed loans records held by ICB in 2018. This illustrates the vastness of the database, which processes the personal data of 2.8 million data subjects. As outlined above, the gravity of the infringement was severe, and a large number of data subjects were affected, despite the fact that the number was relatively low in the context of the total number of closed loan records held by the ICB. This highlights the importance of dissuading future non-compliance. I have also had regard to the negligent character of the infringement and the sensitive category of personal data processed on the database. It is clear that non-compliance with Article 25(1) poses a significant threat to the rights and freedoms of the data subjects whose personal data is processed on the ICB's database. Furthermore, I consider that a fine is also necessary when considered in light of the need to achieve general deterrence and in ensuring that the ICB

[37] ICB submissions on the Draft Decision, dated 23 February 2021, at page 22.

and other controllers operating databases with sensitive personal data are adequately dissuaded from non-compliance with Article 25(1) of the GDPR. Therefore, an administrative fine is effective and proportionate in re-establishing compliance and in dissuading the ICB from failing to comply with its on-going obligations under article 25(1).

9.47 In making this decision to impose an administrative fine, I have had regard to the reprimand made in this Decision. I have also had regard to all of the factors under Article 83(2)(a) – (j). While the reprimand formally acknowledges the serious nature of the infringement of Article 25(1) and is of utility in providing an effective and dissuasive response, I find that the reprimand alone is not sufficient to pursue the objective of re-establishing compliance. I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. In light of the nature of the ICB's database and the ongoing obligation under Article 25(1) in respect of that database, I find that an administrative fine, in addition to the reprimand, is effective, proportionate and dissuasive with a view to re-establishing compliance and ensuring that the ICB continually maintains its obligations under that article.

9.48 Regarding the infringement of Articles 5(2) and 24(1) of the GDPR, I have had regard to how the ICB's failure to maintain a documented record of the testing undertaken in respect of coding changes to the ICB's database not only prevented the ICB from demonstrating its compliance, but also prevented the DPC from assessing the adequacy of the testing actually undertaken in respect of the coding change. I have balanced this with the moderate gravity of the infringement and how the ICB has since undertaken a review of its testing methodology. I have also had regard to the dissuasive effect of the reprimand in this Decision, which, in the circumstances of this case, I find is effective, proportional and dissuasive in respect of this infringement without the need for an additional administrative fine. Therefore, I do not propose to impose an administrative fine in respect of the ICB's infringement of Articles 5(2) and 24(1) of the GDPR.

ii. The Permitted Range

9.49 Having decided that the infringement of Article 25(1) warrants the imposition of an administrative fine in the circumstances of this case, I must next proceed to decide on the amount of that fine. First, it is necessary to consider the appropriate cap for the fine as a matter of law. The cap determines the permitted range for the fine, from a range of zero to the cap. However, the cap is not a starting point for a fine. After identifying the permitted range, it is necessary to calculate the fine.

9.50 Article 83(4) of the GDPR provides that infringements of the obligations of controllers pursuant to, amongst others, Article 25(1) shall:

> *"…in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher…"*

9.51 The turnover of the ICB in 2020 was [redacted] as submitted by the ICB in its submissions on the Draft Decision, and which reflects the ICB's latest Management Accounts. As regards the maximum amount for the fine that may be imposed in this case, the relevant cap for any fine in respect of an infringement of Article 25(1) is the higher of €10,000,000 or 2% of the annual turnover of the preceding financial year. Therefore, I am satisfied that the cap for the ICB's infringement is €10,000,000. 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.

iii. Calculating the Administrative Fine

9.52 In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[38]. The methodology that I have followed is intended to clearly and unequivocally set out the elements taken into account in calculating the fine, thereby allowing the ICB, as the addressee, to understand the basis for the fine and ensuring that the fine is calculated in a rational manner.

9.53 The methodology that I have followed in calculating the administrative fine is as follows. The first step in calculating the administrative fine is to consider the permitted range and to locate the infringement on that permitted range. In this regard, the cap provided for in Article 83(4) is not a starting point for the fine. Rather, it is relevant to determining the permitted range. The determination of where on the permitted range the appropriate figure lies is made by reference to nature, gravity, and duration of the infringement, as considered in relation to Article 83(2)(a) above, and the other aggravating factors. The determination is made in the context of the objectives of re-establishing compliance, including through deterrence, and to provide a proportionate response to the unlawful behaviour. The second step in calculating the administrative fine is to apply the mitigating factors to reduce the fine where applicable. Finally, the third step is to consider whether the figure arrived at is *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR.

9.54 The Draft Decision set out a proposed range for the administrative fine and the factors to be considered, and the methodology to be used when calculating the fine, in order to provide the ICB with the opportunity comment in accordance with fair procedures. In its submissions on the Draft Decision, the ICB submitted that the gravity of the infringement was not severe, and rather that it was moderate to minimal. The ICB also submitted that the DPC was incorrect to treat the negligent character of the infringement and the sensitivity of the personal data affected as aggravating factors pursuant to article 83(2)(b) and (g). For the reasons set out above in my consideration of article 83(2) (a), (b) and (g), I do not accept these submissions. However, I accept the ICB's submission that the specific issues giving rise to the finding of the infringement of Article 25(1) in this Decision have now been addressed by the ICB. I have also had due regard to the up to date financial position of the ICB in calculating the fine, as submitted by the ICB in its submissions on the Draft

[38] See by analogy Electrabel v Commission, T 332/09, ECLI:EU:T:2012:672, para 228, Marine Harvest ASA v Commission, T-704/14, ECLI:EU:T:2017:753, para 450.

Decision. The ICB also submitted that additional credit should be applied towards mitigation. I have had regard to those submissions in assessing the factors in Article 83(2)(a) – (k) above and I have increased the mitigating value where appropriate as detailed below.

9.55 As outlined above, the permitted range for the infringement of Article 25(1) is up to €10,000,000. In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement and the sensitivity of the personal data affected by the infringement as assessed in accordance with Article 83(2)(b)&(g) above. I have also had regard to the up to date economic situation of the ICB. I find that the figure of €220,000 is appropriate in the circumstances of this case before applying mitigation.

9.56 I find that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(c), 83(2)(e), and 83(2)(f) of the GDPR mitigating. To account for the action taken by the ICB to mitigate the damage suffered by the data subjects, I have reduced the fine by €55,000 in accordance with Article 83(2)(c). To account for the ICB's lack of previous infringements, I have reduced the fine by €25,000 in accordance with Article 83(2)(e). In relation to the ICB's cooperation with the DPC to remedy the infringement and to mitigate its adverse effects, I have revised the mitigation value that was proposed to reflect the ICB's latest submissions on the Draft Decision. As outlined above, I accept that the ICB has shown a high degree of cooperation, including by implementing a comprehensive change management process that provides for testing and a formal approval procedure for coding changes. I have reduced the fine by €50,000 to reflect this in accordance with Article 83(2)(f). Thus, the total reductions in light of the mitigating factors is €130,000. Therefore, the final figure for the administrative fine is €90,000.

9.57 The final step is to consider whether the figure arrived at is *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR. I consider that the figure of €90,000 meets these requirements. In order for any fine to be effective, it must reflect the circumstances of the individual case. The circumstances of this infringement concerns the failure to adequately implement appropriate technical and organisational measures designed to implement the principle of accuracy into a database containing sensitive personal data. The resulting personal data breach included 1,062 inaccurate accounts being shared with ICB members and directly with data subjects. The purpose of sharing the records with ICB members was to assist those financial institutions' consideration of applications for credit. I consider that these circumstances require a significant fine in order for it to be effective. In order for a fine to be dissuasive, it must dissuade both the controller/processor concerned, as well as other controllers/processors operating databases with sensitive personal data, from repeating the conduct concerned. I am satisfied that the figure would be dissuasive to both the ICB and to other controllers and processors. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of the fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the figure of €90,000 for the fine does

not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR. The figure of €90,000 amounts to 0.9% of the cap available and 2% of the ICB's turnover. Accordingly, I am satisfied that the amount of the fine is effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

10. Right of Appeal

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

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

The Case Officer delivered the Final Inquiry Report to me on 10 September 2020. I also had regard to all of the correspondence, submissions, and documentation gathered during the Inquiry and the decision-making stage, including:

(i) The DPC's Final Inquiry Report, Inquiry Reference IN-19-7-2;
(ii) Documentation concerning the breach notification BN-18-9-45, including the breach notification form and updates, the emails between the ICB and DPC;
(iii) The ICB Members' Technical Manual, dated August 2018;
(iv) The ICB Members' Technical Manual, dated July 2015;
(v) The Irish Credit Bureau Change Request – PP Update, dated 28 June 2018;
(vi) The Irish Credit Bureau Change Request – PP Update – C and T fix, dated 30 August 2018;
(vii) Standard ICB membership contract and GDPR Compliance Amendment Agreement;
(viii) Redacted email from an ICB member to the ICB, dated 27 August 2018, that gave rise to the ICB's investigation that led to the discovery of the personal data breach;
(ix) Standard ICB Amendment to Terms of Membership, dated 2018;
(x) Data Protection Commission Regulatory Investigator's note of phone call with the ICB, dated 26 October 2018 at 11 am;
(xi) ICB GDPR Fair Processing Notice, dated 23 February 2018;
(xii) ICB Records of Data processing Activities, dated 3 May 2018;
(xiii) DPC Notice of Commencement of an Inquiry, dated 19 July 2019;
(xiv) The ICB's Response to the Commencement letter, dated 15 August 2019, including the *"Queries and Answers"* document;
(xv) ICB internal email, dated 31 August 2018, titled *"Issue with 'C' and the latest balance date"*;
(xvi) ICB internal email thread, dated between 4 - 6 September 2018, titled *"Data related to recent data integrity breach"*;
(xvii) ICB internal email, dated 6 September 2018, titled *"BOICC purge date query"*;
(xviii) Blank ICB Data Protection Impact Assessment (DPIA) for Irish Credit Bureau DAC;
(xix) ICB GDPR Awareness Training for PI Team slides, dated March 2018;
(xx) BSI Certificate of GDPR training, dated 10 October 2019;
(xxi) BSI EU GDPR Foundation Level Training slides, undated;
(xxii) Certification Europe, Irish Credit Bureau Surveillance Assessment Report ISO 27001:2013, dated 26 April 2018;
(xxiii) Letter from DPC to ICB, dated 19 November 2019, posing additional queries;
(xxiv) ICB Response to the additional questions from DPC on inquiry IN-19-7-2, received 3 December 2019;
(xxv) PWC GDPR Readiness Assessment Report in respect of the ICB, dated June 2017;
(xxvi) ICB document titled *"ICB Implementation of the PWC recommendations in their GDPR Readiness Assessment Report June 2017"*;
(xxvii) Letter from DPC to ICB, dated 11 March 2020;

(xxviii) ICB Response to the additional questions from DPC on inquiry IN-19-7-2, received 24 March 2020;

(xxix) Irish Credit Bureau Sample Credit Report;

(xxx) The ISO's "*Code of practice for information security controls"* ,ISO/IEC 27002:2013(E), Second edition, 2013-10-01;

(xxxi) The ISO's *"Information security risk management"* ISO/IEC 27005:2018(E), Third edition, July 2018;

(xxxii) Complaint C-18-8-133 form received by the DPC and related correspondence;

(xxxiii) ICB Training Manual for End User Training, dated 18 May 2018;

(xxxiv) DPC letter to ICB, dated 23 July 2020, enclosing the Draft Inquiry Report;

(xxxv) DPC Draft Inquiry Report, Irish Credit Bureau DAC, Inquiry Reference: IN-19-07-02, Report Issued 23 July 2020;

(xxxvi) ICB submissions on the Draft Inquiry Report, dated 20 August 2020;

(xxxvii) ICB document, titled *"A12 Operations Security"*, dated 15 December 2020; and

(xxxviii) Email from the ICB to the DPC enclosing its submissions on the Draft Decision, dated 23 February 2021;

(xxxix) ICB submissions on the Draft Decision, titled *"Response to Draft Decision 02 February 2021"*, dated 23 February 2021;

(xl) The ICB's original change control and testing policies, in place June – August 2018 (appendix 1 to the ICB's submissions on the Draft Decision);

(xli) The ICB's change control and testing policies post 20 August 2020 (appendix 2 to the ICB's submissions on the Draft Decision);

(xlii) The ICB's Operations Security Policy, *"ISO27001:2013 Reference A12 Operations Security"*, Rev 1.7, dated 15 December 2020;

(xliii) The ICB's Change Management Policy, Rev 1.4, dated 17 February 2021;

(xliv) The ICB's DPIA Template, submitted as part of appendix 3 to the ICB's submissions on the Draft Decision;

(xlv) The ICB's Systemic Change Control document, Rev 1.5, dated 18 February 2021;

(xlvi) The ICB's Organisational Change Control document, Rev 1.5, dated 18 February 2021;

(xlvii) The ICB's Change Request Control Log detailing 1 September 2020 – 7 December 2020;

(xlviii) The ICB's Implementation Plan Template, Rev 1.2, dated 11 February 2021;

(xlix) The ICB's Testing Policy and Procedures, Rev 1.7, dated 18 February 2021;

(l) The ICB's Test Plan Template, Rev 1.1, dated 11 February 2021; and

(li) The ICB's Test Case Template, submitted as part of appendix 3 to the ICB's submissions on the Draft Decision.