In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-7-5

In the matter of Slane Credit Union Limited

Decision of the Data Protection Commission under Section 111 of the Data Protection Act 2018

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

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

26 January 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Purpose of this document

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 authorised officers of the DPC (the "**Inquiry Team**") pursuant to Section 110 of the 2018 Act. The Inquiry Team provided Slane Credit Union Limited ("**SCU**") with a draft inquiry report on 20 March 2020 (the "**Draft Inquiry Report**") and a final inquiry report on 14 October 2021 (the "**Final Inquiry Report**").

1.2. SCU was provided with the Draft Decision in this Inquiry on 22 December 2021 to provide it with a final opportunity to make submissions. This Decision is being provided to SCU pursuant to Section 116(1)(a) of the 2018 Act in order to give SCU notice of the Decision, the reasons for it, and the corrective powers that I have decided to exercise.

1.3. This Decision contains corrective powers under Section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (Regulation (EU) 679/2016) (the "**GDPR**") arising from the infringements that have been identified herein. In this regard, SCU will be required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on SCU 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 ("**EU**"). The GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to Section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on 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 the Inquiry is provided for under Section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to carry out an independent assessment of all the materials provided to me by the Inquiry Team as well

as any other materials which have been furnished to me by SCU, and any other materials which I consider to be relevant, in the course of the decision-making process.

2.4. The Final Inquiry Report was transmitted to me, together with the Inquiry Team's file, containing copies of all correspondence exchanged between the Inquiry Team and SCU; and copies of all submissions made by SCU, including the submissions made by SCU in respect of the Draft Inquiry Report. SCU made submissions on the Draft Decision on 21 January 2022.

2.5. Having reviewed the Final Inquiry Report, and the other materials provided to me by the Inquiry Team, including the submissions made by SCU, 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, opportunities for the controller to comment on the Draft Inquiry Report before it was submitted to me as decision-maker, and that the powers exercised by the Inquiry Team were lawfully invoked.

3. Factual background

i. Controller overview

3.1. SCU was established on 16 February 1968 as a member of the Irish League of Credit Unions. SCU is regulated by the Central Bank of Ireland under section 84 of the Credit Union Act 1997.

3.2. SCU is a financial co-operative that provides savings and loan facilities for the benefit of its members. SCU offers financial services on a not for profit, member-owned basis and it has a current membership in the region of 3,500 members, with five permanent staff and 11 directors.

ii. Personal data breach and notification

3.3. On 30 November 2018 (the "**Date of Notification**"), the DPC received a personal data breach notification from SCU (DPC reference number BN-19-12-27) (the "**Breach Notification**"). The issue notified related to an unauthorised disclosure of personal data in the form of an unintended publication of member data on the internet (the "**Personal Data Breach**"). Certain reports relating to membership enquiries ("**Member Enquiry Reports**") were stored within the directors' area (the "**Directors' Area**") of the www.slanecreditunion.ie website, which is owned and operated by SCU. After an investigation, SCU determined that the technical configuration of the website inadvertently allowed four Member Enquiry Reports to be searchable online from the 21 or 22 November 2018 until the 29 November 2018.[1] According to SCU, this incident occurred due to an update to a search engine optimisation tool installed on the website that SCU had not anticipated. As of 29 November 2018, Member Enquiry Reports dating back to 2015 were stored in the Directors' Area.

iii. Impact of the Personal Data Breach

3.4. The categories of personal data affected by the Personal Data Breach were the names; addresses; gender; dates of birth; and SCU account numbers, opening dates and types of 76 members of SCU.[2] 34 of those members were children. In the Breach Notification, SCU assessed the likelihood of a risk arising to the rights and freedoms of those data subjects as

[1] Letter of 4 November 2021 and Breach Notification Form submitted by SCU to the DPC in November 2018

[2] Redacted sample of one of the Member Enquiry Reports affected by the Personal Data Breach provided to the DPC on 23 December 2019

"high," and marked some of the potential consequences as being: loss of control of the personal data, identity theft and fraud.

3.5. In the Breach Notification, SCU ticked a box indicating that economic or financial data had been disclosed in the Personal Data Breach. On 22 May 2020, SCU confirmed that this box had been ticked inadvertently, and that no economic or financial data had been disclosed. They further outlined: "however the data released could, admittedly, with intense and concentrated effort be used in an illegal and/or unethical manner." On 4 November 2021, SCU confirmed that "A third party could not use this data to access an account or to successfully make representations to Slane Credit Union, purporting to be the member or representing the member."

3.6. In the Breach Notification, SCU had said that it was impossible to determine if and by whom the reports were accessed as a result of the Personal Data Breach. However, SCU confirmed on 10 January 2019 that malicious activity hadn't been detected in the raw files or the website. SCU had also contacted another of their service providers, who confirmed that there had been no leak of personal data via memberaccess or SCU's locally hosted SQL database server.

iv. Breach response

3.7. SCU acted immediately to identify the cause of the Personal Data Breach and by liaising with service providers and search engines to put an end to the breach. Subsequently, they made a number of changes to the process by which Member Enquiry Reports were circulated to directors, and the duration for which those reports were stored on the Directors' Area. They also compiled an incident report for the Personal Data Breach. Full details of the mitigating steps taken by them are set out in paragraphs 9.32 to 9.40.

v. Inquiry IN-19-7-5

3.8. The DPC issued a letter to SCU on 19 July 2019 notifying it of the commencement of an inquiry under section 110(1) of the 2018 Act (the "**Inquiry Commencement Notice**"). During the course of the Inquiry, SCU also replied to written questions sent by the Inquiry Team. An onsite inspection was arranged for 9 December 2019, at which authorised officers of the DPC attended SCU's offices. The Manager and the Processor were both in attendance at that inspection. The Final Inquiry Report noted that both individuals cooperated with the Inquiry Team, provided replies to the questions posed and agreed to supply further supporting information.

3.9. The Draft Inquiry Report was issued to SCU on 20 March 2020. SCU furnished their submissions on the Draft Inquiry Report and the Final Inquiry Report was issued to SCU on 14 October 2021.

vi. Commencement of decision-making

3.10. On 14 October 2021, a notice of commencement of decision-making was sent to SCU and on 22 December 2021, the Draft Decision was sent to SCU. SCU sent submissions on the Draft Decision on 21 January 2022.

4. Scope of the Inquiry

4.1. The scope of the Inquiry set out in the Inquiry Commencement Notice was to examine whether or not SCU 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 or the GDPR had been contravened by SCU in that context.

4.2. The Personal Data Breach concerned the unauthorised disclosure of personal data from the Directors' Area of the www.slanecreditunion.ie website, owned and operated by SCU. I am satisfied that SCU fulfils the role of controller within the meaning of Article 4(7) of the GDPR in circumstances where it determines the purposes and means of processing on its website.

5. Issues for determination

5.1. Having reviewed the Final Inquiry Report and the other materials provided to me, I have determined the issues in respect of which I must make a decision. The issues that I have determined fall for consideration are whether SCU complied with the following obligations, between 25 May 2018 and 30 November 2018 (the "**Temporal Scope**") in respect of the personal data of members of SCU on the Directors' Area in the form of Member Enquiry Reports (the "**Member Personal Data**"):

1) Articles 5(1)(f), and 32(1) of the GDPR, which require controllers to implement appropriate technical and organisational measures to ensure the appropriate security of the personal data;

2) Articles 24(1) and 30(1) of the GDPR, which require controllers to ensure that processing is in accordance with the GDPR, and to put in place a record of processing activities that contains certain specified information; and

3) Article 28 of the GDPR, which requires controllers to engage processors who put in place sufficient guarantees for the protection of personal data, and to put in place an agreement with processors containing certain specified clauses.

6. Issue 1: Whether SCU infringed Articles 5(1)(f) and 32(1) of the GDPR in relation to Member Personal Data during the Temporal Scope

6.1. Article 5(1)(f) of the GDPR sets out the principle of integrity and confidentiality. It requires that personal data shall be:

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

6.2. Article 32(1) of the GDPR elaborates on the principle of integrity and confidentiality. It sets out criteria for assessing what constitutes "appropriate technical and organisational measures," stating:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and*

severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

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

6.3. Thus, Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data.

i. Assessing Risk

6.4. In determining the appropriate technical and organisational security measures, the first step that a controller must take is to assess the risk presented to the rights and freedoms of data subjects by the processing of personal data, and then to assess the appropriateness of the security measures implemented.

6.5. Recital 76 of the GDPR provides guidance on how this risk can be assessed, stating,

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.

6.6. The CJEU judgment in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[3] provides further guidance on the risk assessment. In that case, the CJEU declared the Data Retention Directive[4] invalid. That Directive required electronic communication service providers to retain certain data for a period of time. The CJEU held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to:

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

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

(i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.[5]

6.7. Considering the CJEU approach, it appears that risk is assessed objectively by reference to (a) the likelihood of the risk, and (b) the severity of that risk to the rights and freedoms of natural persons. Those objective assessments must be made by reference to the nature, scope, context and purposes of the processing. In considering those factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data.

6.8. With respect to the scope and context of processing of Member Personal Data by SCU, this involved the uploading of Members Enquiry Reports to the Directors' Area for access and review by directors of SCU at, and in advance of, board meetings. The purposes of this processing were for directors to review new member applications, with the SCU's submissions on 22 May 2020 stating, "It is only by obtaining the application details that the board can fulfil their legal obligation."

6.9. The Member Personal Data included the names, addresses and dates of birth of data subjects, and information relating to the fact of their membership of SCU. With respect to the nature of this data, it does not fall into a special category of personal data,[6] and it does not include financial data. However, the personal data affected by the Personal Data Breach did include the personal data of child members of SCU. Children merit specific protection with regard to their personal data under the GDPR.[7]

6.10. In relation to the quantity of personal data processed, Member Enquiry Reports dating back to 2015 were stored on the Directors' Area at the Date of Notification. On average, the Member Enquiry Reports contained the details of 19 members.[8] The Personal Data Breach led to the disclosure of four of those Member Enquiry Reports which contained the personal data of 76 members, including 34 children.

(a) Likelihood of risk

6.11. In relation to the technical measures applicable to the SCU website, I note that a plugin had been installed on the website to ensure search engine optimisation. Based on the description of the circumstances leading to the Personal Data Breach provided by SCU, the installation of that tool on the SCU website created a risk of the inclusion of Member Personal Data in search engine results unless steps were taken to ensure that the tool or the website more generally was correctly configured. In that regard, I note that the www.slanecreditunion.ie website was not updated or checked regularly, and the search engine optimisation tool had not been updated since first use in 2015. Moreover, at the Date

[5] Digital Rights Ireland (op. cit.), [66]
[6] As defined in Article 9(1) of the GDPR
[7] Recital 38 of the GDPR. See also the specific protections provided for in Articles 6(1)(f) and 8 of the GDPR.
[8] Data Protection Risk Assessment and Data Protection Impact Assessment provided to DPC on 4 November 2021

of Notification, SCU did not have a system monitoring or change management policy in place in relation to the website.

6.12. Unauthorised disclosure in itself presents risks to data subjects, as it leads to data subjects losing control over their personal information. As regards the likelihood of any specific harm arising from that unauthorised disclosure, I note that the personal data in Member Enquiry Reports included names, addresses, and dates of birth. SCU confirmed that it would not be possible to use that personal data to access an account or successfully make representations to SCU purporting to be the member or representing the member. Thus, there does not appear to be a financial risk arising from a breach of security affecting the Member Personal Data, at least insofar as each member's credit union account is concerned. However, that personal data does create a risk of identity theft and fraud. As highlighted by guidance from the UK Information Commissioner's Officer "Your name, address and date of birth provide enough information to create another 'you.'"[9] Those details could be used to make attempts to impersonate data subjects in an effort to retrieve other personal information about them, and could also be used in a hacking attempt or to set up false accounts in a data subject's name. A recent study commissioned by the European Commission shows that Ireland is one of the EU countries with the highest incidences of identity theft and fraud. 50% of respondents in Ireland said that they had experienced identity theft in the two years preceding the study (2017-2019).[10] However, the majority of frauds and scams were experienced through online channels or over the phone, and only 4% of scams in the EU took place via postal letter.[11]

6.13. Based on this analysis, the personal data in Member Enquiry Reports does entail some risks for data subjects. In a technical sense, the likelihood of an unauthorised disclosure occurring is high, considering the lack of oversight that was in place over the Directors' Area during the Temporal Scope. In relation to the likelihood of harm to data subjects, however, there appears to be a moderate risk that someone could use the personal data in Member Enquiry Reports to cause harm to data subjects in one of the ways outlined above. On balance, therefore, I consider the likelihood of risk to data subjects arising from the processing of Member Personal Data during the Temporal Scope to be moderate.

(b) Severity of risk

6.14. As noted, the personal data in Member Enquiry Reports did not contain any special category or financial data. However, it did include children's data and also related to private aspects of members' lives. As noted above, the disclosure of personal data in Member Enquiry Reports could also lead to a risk of identity theft. In the EU Commission survey mentioned above, of the respondents who had suffered any type of fraud or scam, 24% said

[9] ICO, *Identity Theft*, available at https://ico.org.uk/your-data-matters/identity-theft/ (accessed 24 January 2022)

[10] Ipso, *Survey on 'Scams and Fraud Experienced by Consumers: Final Report*, published by the European Commission, January 2020, available at survey on scams and fraud experienced by consumers - _final_report.pdf (europa.eu) (accessed 10 December 2021), 13

[11] Ibid, 31

they had suffered financially, and 6% suffered physically. A very high percentage – 79% – experienced emotional suffering as a result of fraud or scam.[12]

6.15. Based on an assessment of these factors, I consider that the severity of the risk to the rights and freedoms of natural persons arising from the processing of Member Personal Data was moderate. This takes into consideration the facts that three years' worth of Member Enquiry Reports were stored on the Directors' Area, the personal data included data of at least 36 children, and it also takes into account the fact that it could lead to identity theft, creating risks of financial harm or emotional distress to data subjects. As mitigating factors, it takes into account the fact that the personal data could not lead to the accessing of a credit union account, and did not include financial data or special categories of personal data.

ii. Security measures implemented by SCU

6.16. In implementing appropriate security measures, the obligation falls on the controller to first consider the risk presented to the rights and freedoms of natural persons by the relevant processing of personal data. Having assessed this risk, the controller must then implement measures that are appropriate in light of the risk.

6.17. SCU have provided details of the technical and organisational measures in place on the www.slanecreditunion.ie website at the Date of Notification.

I. Technical measures

6.18. The website was constructed using a Wordpress application and hosted on a domain called www.webshost.ie. The Directors' Area was a password protected section of that website. Each director of SCU had been emailed a password for the Directors' Area in 2015 just before the www.slanecreditunion.ie website was launched. Those passwords could not be changed by directors. Each month, the general manager of SCU (the "**Manager**") emailed a board pack to an outsourced service provider and sole trader who SCU had engaged to design and manage the www.slanecreditunion.ie website (the "**Processor**"). The Processor would then email the board pack to another service provider based in another EU member state (the "**Sub-Processor**"), who was the only person with administrator access to the www.slanecreditunion.ie website.[13] In turn, the Sub-Processor uploaded the board pack to the Directors' Area, and directors could log in and view the uploaded materials. A data processing agreement between SCU and the Processor was signed on 31 October 2015 (the "**2015 DPA**"). There was no data processing agreement in place between SCU and the Sub-Processor, or between the Processor and the Sub-Processor.

6.19. A plugin provided by Yoast was applied to the website, the functions of which were described by SCU as including search engine optimisation and the non-indexing of URLs that they did not want to be indexed by search engines.[14] According to SCU, the Personal Data Breach was caused by an update to the Yoast plugin which took place on 21 or 22 November 2018. They claimed the update had the effect that a "noindex" setting which had been applied to the Directors' Area unset, leading to the indexing of certain files stored in the Directors' Area on search engines. SCU said that this issue was discovered by a staff member

[12] Ibid, 16
[13] Website Design Brief, 8 June 2015
[14] Letter of 15 August 2019

who had run a search on www.google.com in relation to rental properties in Slane. The staff member notified the Manager of this issue on 29 November 2018.

6.20. SCU said that the Yoast plugin had not been updated by them since first use in 2015, and that it had functioned correctly and without problems until the update on 21 or 22 November 2018, which SCU described as being unannounced. They also said that the website was not checked regularly for updates or security checks. The Final Inquiry Report concluded that,

> *The controller cannot demonstrate with any supporting documentation how the default web site privacy settings were enabled from the outset in 2015. The controller acknowledges that it was not aware of any updates nor was any regular review conducted in relation to any security updates*.[15]

II. Organisational measures

6.21. SCU provided information about the IT policies applicable to its website at the Date of Notification. On 21 May 2018, an ICT acceptable use/electronic communications policy and a password standards policy were adopted by SCU. SCU also sent the DPC a presentation on IT training that had been provided to them by a service provider. A Data Breach Policy and Procedure was adopted by SCU on 21 May 2018, which sets out details of the procedures to be followed in respect of all personal data on SCU's ICT systems. It contains a template data security breach report, which was used by SCU to record details of the Personal Data Breach.

6.22. SCU confirmed that they did not have a system monitoring policy in place at the Date of Notification.[16] SCU also failed to produce any written change management procedures that were in place at that time.[17] They said that instruction for changes to the website was given by the Manager. Vulnerability testing was carried out occasionally. They confirmed that the board of directors was responsible for decisions on technical and organisational measures, and that advice was sought by them in written and verbal form. On 17 January 2019, SCU acknowledged that more formality was required for the website.

6.23. A website design brief and management agreement between the Processor and Sub-Processor dated 8 June 2015 were provided to the DPC. On 4 November 2021, SCU confirmed that the security measures applicable to the Directors' Area as of the Date of Notification were those set out in the website design brief of 8 June 2015. In that document, the Processor gives the following instructions to the Sub-Processor in relation to the design of the Directors' Area,

> *Slane want a Directors Area that will be secure. Board reports will be loaded to these pages so must be very secure. Each Director will be have a username and login in created by you … and sent to the manager of the Credit Union through me. Once the emails are sent you and I will delete these emails so that you and [the Manager] are the only ones who know what the access codes are. You will be the only admin of the website until we hand it over.*

[15] Final Inquiry Report, [94]
[16] Ibid, [95]
[17] Ibid, [100]

Directors will not be allowed change access details and they won't have a save option. [The Manager] will send me the initial Board packs which I will forward to you. Again, all emails and downloads will be deleted (I won't open them as I don't have any interest in the contents) once they are uploaded.

…

The website needs to track logins, failed logins and use of false usernames. Anyone using false usernames need to be blocked.

If logins fail the Director will have to ask the manager of Slane to unblock them. Whoever will manage the website after it is completed needs to be able to permanently block them.[18]

6.24. There is no reference to personal data being processed on the Directors' Area in that section of the document. In a subsequent section called "Data Protection," the website design brief says, "The site will not collect data from clients other than contact details and will be connected to email." Thus, the website design brief does not consider the processing of Member Personal Data in the Directors' Area. Consequently, it does not take account of the severity or likelihood of risks to the rights and freedoms of natural persons arising from the processing of Member Personal Data. A Data Protection Report dated 25 November 2016 was supplied by SCU, too. It also states that the Directors' Area does not contain personal data.[19]

6.25. Aside from a reference to a search engine optimisation tool in the Website Design Brief, there is no documented material about the use of the plugin, or any assessment of whether this would cause a risk to the Directors' Area. The analysis in the design specification was not updated to take account of the requirements of the GDPR, and it was confirmed by SCU on 4 November 2021 that it was still the most relevant document about the architecture of the www.slanecreditunion.ie website as of the Date of Notification. SCU said that the Yoast plugin was chosen for the website as it provided a number of features in one plugin, including control of meta titles and tags, to enable and maintain the website sitemap, and to have control over search engine indexing. SCU did not carry out a review of alternatives to that plugin.

iii. The appropriate level of security

6.26. An appropriate level of security includes both technical and organisational measures. Technical measures must have, *inter alia*, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Organisational measures should enable controllers to test, assess and evaluate the effectiveness of those technical measures.[20]

6.27. Having regard to the moderate severity and likelihood of the risk to the rights and freedoms of data subjects, an appropriate level of security of Member Personal Data during the Temporal Scope included:

[18] The wording has been amended to remove the names of specific individuals.
[19] 7 at para [11.h]
[20] Article 32(1)(d) of the GDPR

a) An assessment that considered:

- the nature, scope, purposes and context of processing personal data on the Directors' Area and the likelihood and severity of the risks to the rights and freedoms of natural persons arising from that processing; and
- the technical and organisational measures that would ensure the confidentiality, integrity, availability and resilience of that personal data.

b) Putting in place the technical and organisational measures identified in the risk assessment outlined at (a).

c) Putting in place a system for the regular testing, assessment and evaluation of the effectiveness of the measures put in place pursuant to (b).

6.28. As of the Date of Notification, SCU had not assessed the likelihood or severity of risks to Member Personal Data. Indeed, its website policies did not even acknowledge the fact that Member Personal Data was processed on the Directors' Area. Moreover, although some security measures had been implemented on the Directors' Area, those security measures were not regularly tested or evaluated for efficacy. The result was that Member Personal Data was affected by the Personal Data Breach and became listed in search engine results for a period of time leading to the Date of Notification.

Conclusion on Issue 1: I find that SCU infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of Member Personal Data.

7. Issue 2: Whether SCU infringed Articles 24 and 30(1) of the GDPR in relation to Member Personal Data during the Temporal Scope

7.1. Controllers are responsible for demonstrating and monitoring compliance with the GDPR. This general principle is set out in Article 5(2) of the GDPR, and is given further effect by Article 24, the first two subparagraphs of which read,

> *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.*

7.2. Article 30(1) of the GDPR requires controllers to maintain a record of processing activities, containing the following information:

> *(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

7.3. Thus, Articles 24 and 30(1) both envisage the implementation by controllers of certain policies and records. It is clear from the listed criteria set out in Article 30(1) for inclusion in a record of processing, and from the specific factors to which a controller must have regard under Article 24(1) that those provisions envisage the accurate identification by the controller of the nature of personal data processed by them, in addition to the purposes for which they are processed. Consequently, in order to meet the requirements of those provisions, and to effectively demonstrate compliance with the GDPR, a controller's data protection records and policies must accurately reflect the processing of personal data by that controller. In that vein, they must be maintained as living documents that are updated to take account of any developments to the processing operations of the controller.

7.4. By the Date of Notification, SCU had adopted a number of data protection policy and procedure documents that sought to reflect some requirements of the GDPR, which began to apply earlier that year. These include a data inventory, data protection policy, data breach register and a records management and retention policy dated 21 May 2018.[21]

7.5. SCU also provided a blank copy of an activity pack and workbook called "Managing the GDPR in Credit Unions" and a blank "GDPR Assessment for Credit Union 2019." SCU said that annual training was organised. They provided a training sign-in sheet from 7 April 2019, signed by ten employees. On 4 November 2021, SCU also provided screenshots showing completion by SCU staff and directors of data protection training on CU Learn.

7.6. It is commendable that SCU took steps to put those policies in place. However, as was noted in the Final Inquiry Report, the data inventory, which was put in place in order to seek to ensure compliance with Article 30 of the GDPR, did not accurately reflect the data processing taking place.[22] Neither did it document why the new member account details would need to be disclosed to the directors, nor a time limit for the retention of that personal data.[23] Thus,

[21] The date of these documents was confirmed by SCU on 4 November 2021
[22] Final Inquiry Report, [100]
[23] Ibid, [104]

the full details required by Article 30(1) of the GDPR were not included in that record of processing. More generally, SCU's policy documents do not contain any specific reference to the processing of Member Personal Data on the www.slanecreditunion.ie website. Having regard to the nature, scope, context and purposes of that processing, outlined in more detail in Section 6, I find it was proportionate for SCU's data protection policies to have included a reference to that processing.

7.7. A failure to put in place correct policies and records can have knock-on consequences for ensuring compliance with the GDPR. If SCU's documents had identified the processing of Member Personal Data on the Directors' Area, it may have led to a consideration of the necessity for processing Member Personal Data on that area, or a re-evaluation of whether appropriate technical and organisational security measures were in place.

7.8. In these ways, the policies that SCU had in place during the Temporal Scope did not take full account of the nature, scope context and purposes of processing by SCU. As a consequence, those policies do not demonstrate compliance by SCU with the GDPR in respect of Member Personal Data. Its data inventory did not contain details of Member Personal Data, and thus failed to fully meet the requirements of Article 30(1) of the GDPR.

Conclusion on Issue 2: I find that SCU infringed Articles 24 and 30(1) of the GDPR by failing to implement organisational measures that take account of the nature, scope, context and purposes of its processing, and by failing to include references to Member Personal Data in its data inventory.

8. Issue 3: Whether SCU infringed Article 28 of the GDPR in relation to Member Personal Data during the Temporal Scope

8.1. Under Article 28(1) of the GDPR, controllers:

> *shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

8.2. In their submission on the Draft Inquiry Report, SCU said,

> *Not abrogating responsibility Slane Credit Union relies on the professional ability of its outsource providers such as risk/compliance, internal audit and technical suppliers. We believed that the interaction of these functions provided a legislative safety net to Slane Credit Union.*[24]

8.3. Processors cannot be used by controllers as a legislative safety net, and it is essential that due diligence is carried out to ensure that processors provide sufficient guarantees to implement appropriate technical and organisational measures for the protection of personal data, in line with Article 28(1). SCU have not provided any evidence that they carried out due diligence on the Processor in relation to the Processor's data protection credentials, and based on the information collected during the Inquiry, it does not appear that the Processor

[24] Quoted in the Final Inquiry Report, [65]

did, in fact, put sufficient guarantees in place for the protection of personal data. Based on the analysis of Issue 1, it appears that the Processor did not have regard to the risks to Member Personal Data either in 2015 when the website was first developed, or at any time during the Temporal Scope, when they continued to liaise with the Sub-Processor to upload Member Enquiry Reports to the Directors' Area. The Processor also admitted that there had been no active monitoring of website security or ongoing testing of new releases.[25]

8.4. Under Article 28(3) of the GDPR, processing by a processor "shall be governed by a contract or other legal act." That agreement must be "binding on the processor with regard to the controller" and must set out "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller." The contract shall also,

> *stipulate, in particular, that the processor:*
>
> > *(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*
> >
> > *(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
> >
> > *(c) takes all measures required pursuant to Article 32;*
> >
> > *(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;*
> >
> > *(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*
> >
> > *(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;*
> >
> > *(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;*
> >
> > *(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and*

[25] Final Inquiry Report, [71]

contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

8.5. "Processing" is defined broadly in Article 4(2) as:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

8.6. Article 4(8) defines "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

8.7. The Processor uploaded Member Personal Data to the Directors' Area. This falls within the definition of processing set out in Article 4(2) of the GDPR. This processing was carried out on behalf of SCU by the Processor, who therefore acted as a processor within the meaning of Article 4(8) of the GDPR. As a consequence, it was mandatory for SCU and the Processor to put in place an agreement that reflected the requirements of Article 28(3) of the GDPR.

8.8. SCU put a data processing agreement in place with the Processor in 2015 (the "**2015 DPA**"). The 2015 DPA contained three substantive provisions, as follows:

It is agreed that Slane Credit Union will retain all control of personal data within the definition of the Data Protection Acts 1988 and 2003.

[The Processor] agrees that data will be uploaded to the website as directed by Slane Credit Union and will not collect, process, keep, use nor disclose personal data in any way.

Such files sent to [the Processor] which may contain personal data as may be provided by Slane Credit Union will be destroyed once loaded onto the website.

8.9. SCU furnished copies of agreements with two of their service providers, which had been signed on 28 September 2018 and 4 October 2018, and which were entered into to seek to meet the requirements of Article 28(3) of the GDPR. However, they confirmed that the 2015 DPA with the Processor had not been updated in advance of the Date of Notification. The provisions in that DPA do not include the detail required by Article 28(3) of the GDPR, despite the fact that the Processor processed personal data on behalf of SCU. Therefore, SCU and the Processor should have had a new agreement in place containing all of the required provisions, which should have been effective throughout the Temporal Scope.

Conclusion on Issue 3: I conclude that SCU infringed Article 28 of the GDPR by failing to conduct due diligence on the Processor, in line with Article 28(1), by failing to put in place an agreement with the Processor that included the clauses required by Article 28(3).

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 SCU has infringed Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) of the GDPR. Under Section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with Section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not those findings of infringement 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 Inquiry, and with particular reference to the findings of infringements arising therefrom, I find that the exercise of one or more corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR. 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 SCU in respect of its infringements of Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) of the GDPR; and

b) Article 58(2)(i) – I have decided to impose an administrative fine in respect of the infringement of Articles 5 and 32. The reasons for this are outlined below.

9.4. The Draft Decision proposed to order SCU to bring its processing operations regarding Member Personal Data into compliance with Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) of the GDPR in accordance with Article 58(2)(d) of the GDPR. That provisional order would have required SCU to carry out a documented risk assessment that considered the risks to the processing of member personal data in director board packs and the security measures that are appropriate in respect of those risks. It would also have required SCU to update its data inventory and data protection policy to include a reference to the processing of Member Personal Data in board packs, and to ensure that Articles 28(1) and 28(3) of the GDPR are complied with in respect of any services provided to SCU that entail the processing of member personal data.

9.5. SCU's submissions on the Draft Decision on 21 January 2022 appended a number of documents to purportedly address elements of the provisional order directing that processing be brought into into compliance with the GDPR. Those documents included a GDPR gap analysis identifying actions that SCU should take in order to close identified gaps in GDPR compliance. It confirms on p5 that "SCU no longer include member personal data in the monthly board pack going to the Board." SCU also submitted updated versions of its data

inventory and internal data protection policy. Row 78 of the revised data inventory says, "Personal data is not processed at Board Meetings; anonymity non traceability is always observed." Similarly, paragraph 16.3 of the Data Protection Policy states "Personal data is not processed at Board Meetings; anonymity non traceability is always observed." They submitted a written confirmation from the Data Processor that neither he nor the Sub-Processor "have any personal data which comes under GDPR and that all emails, Board Packs and any communication which may have had personal data have been deleted permanently from all systems, including the website."

9.6. SCU also confirmed that "All suppliers of services that entail the processing or access to members personal data have been required to issue statements of compliance." They submitted copies of correspondence and agreements with a number of suppliers.

9.7. In light of the fact that member personal data is no longer included in board packs, it is not appropriate or necessary for this Decision to make an order pursuant to Article 58(2)(d) of the GDPR.

9.8. Regardless of the decision not to impose an order to bring processing into compliance with the GDPR, it must be noted that the implementation mitigating measures by SCU in relation to Member Personal Data does not relieve SCU of its obligation to continually evaluate the effectiveness of the measures that it puts in place to ensure compliance with the GDPR. Nor does this decision confirm that the documents submitted by SCU comply in every respect with the provisions of the GDPR but rather than they address matters in the scope of this Decision.

A. Reprimand

9.9. I issue SCU with a reprimand in respect of its infringements of Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(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 necessary and proportionate in view of ensuring compliance with the infringed Articles, as it will act to formally recognise the serious nature of all of the infringements. Further, the reprimand emphasises the requirement for SCU to take all relevant steps to ensure future compliance with Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) of the GDPR.

9.10. Recital 148 of the GDPR provides:

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

9.11. Accordingly, 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. In this respect, I consider it necessary and proportionate to impose a reprimand in addition to the administrative fine set out in Part 9B of this Decision.

9.12. I have made this decision having particular regard to the nature of the infringements of the GDPR identified in this Decision. The objective of Articles 5(1)(f) and 32(1) is to ensure that controllers and processors implement a level of security that is appropriate to the risk presented by their processing operations. Articles 24 and 30(1) seek to ensure that controllers have in place appropriate policies, procedures and records for the protection of personal data and Article 24 additionally seeks to ensure that controllers have appropriate technical and organisational measures in place to ensure compliance with the GDPR. Finally, Article 28 seeks to ensure that controllers have appropriate oversight of processors engaged by them, and that they ensure those processors adopt sufficient guarantees for the protection of data subject rights. Non-compliance with any of those provisions can have adverse impacts on the rights and freedoms of data subjects and must be dissuaded. The underlying Personal Data Breach considered in this Decision illustrates the potential harm that can flow from SCU's infringements of these provisions.

9.13. Therefore, I consider that that the formal recognition of the seriousness of the infringements by means of a reprimand is appropriate and necessary to ensure compliance with these Articles, and to dissuade future non-compliance by SCU with its obligations under the GDPR. A reprimand is proportionate in the circumstances where it does not exceed what is required to ensure compliance with the GDPR, taking into account the nature of the infringements and the potential for harm to data subjects.

B. Administrative fine

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

9.15. Only the infringements of certain provisions of the GDPR can lead to the imposition of a fine. Of the provisions that have been identified in this Decision as having been infringed, the ones that can trigger a fine are Articles 5,[26] 28, 30(1) and 32(1) of the GDPR.[27] An administrative fine cannot be imposed for an infringement of Article 24. The infringement of that Article by SCU will therefore not be considered in this section.

i. Whether the infringements warrant an administrative fine

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

[26] Article 83(5) of the GDPR
[27] Article 83(4) of the GDPR

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."

9.17. These criteria are crucial to the decision as to whether or not to impose administrative fines and the amount of any such fines. Therefore, I will now proceed to consider each of these criteria in turn in respect of SCU's infringements of Articles 5(1)(f), 13, 28(1), 28(3), 30(1) and 32(1) of the GDPR.

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>

9.18. I have determined that the Temporal Scope in respect of the infringements of the GDPR in this Decision is from 25 May 2018 to 29 November 2018. Thus, the duration of all of the infringements is six months and four days. For the avoidance of doubt, in relation to

Articles 5(1)(f) and 32(1), this Temporal Scope refers to the technical and organisational measures in place and not to the duration of the Personal Data Breach, which SCU stated lasted for eight or nine days before it was detected.

Nature and gravity of the infringements of Articles 5(1)(f) and 32(1)

9.19. The objective of Articles 5(1)(f) and 32(1) is to ensure that personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur.

9.20. The nature of SCU's infringements of Articles 5(1)(f) and 32(1) involved a failure by SCU to put in place appropriate technical and organisational measures for the risk to personal data on the Directors' Area. It failed to identify that personal data were stored on that area of its website in any of its policies or procedures, and also failed to consider the nature of the risk to that data or the security measures that would be appropriate in respect of the likelihood or severity of risks presented to it. Moreover, SCU did not update its website or check for updates on a regular basis. The personal data stored on that area of the website could be used to engage in identity theft, and it included the personal data of children, which merits specific protection in line with the GDPR. As a result of these infringements, the Personal Data Breach occurred, resulting in the unauthorised disclosure of Member Personal Data, which led to risks for the rights and freedoms of data subjects.

9.21. The gravity of this infringement is moderate in circumstances where the likelihood of the risks to personal data on that section of the website were moderate, and where certain security measures, such as password protection, were in place to seek to protect the contents of the Directors' Area. There is also no evidence that any harm was actually suffered by data subjects as a result of these infringements or the Personal Data Breach.

Nature and gravity of the infringements of Article 30(1)

9.22. The purpose of Article 30(1) of the GDPR is to ensure that controllers have in place a record of processing that accurately identifies the personal data processed by them. A failure to identify all relevant processing activities can have the result that personal data are not processed in compliance with the GDPR, and that appropriate technical and organisational measures are not put in place with respect to the risks to the rights and freedoms of natural persons arising from that processing.

9.23. The nature of SCU's infringement of Article 30(1) amounted to a failure to identify the processing of Member Personal Data in the Directors' Area in its records of processing. As a result, their data inventory also does not fully reflect the processing activities carried out by them.

9.24. The gravity of this breach is light in circumstances where SCU had taken steps to adopt a suite of GDPR-compliant policies and procedures, including a data inventory, and adopted those policies at board level on 21 May 2018. It also introduced data protection training for all of its staff members to bring them up to date on the obligations of SCU under the GDPR. Those factors mitigate against the fact that the data inventory did not fully reflect all of the processing carried out by SCU.

Nature and gravity of the infringements of Article 28

9.25. Article 28 of the GDPR seeks to ensure that controllers have oversight of processors engaged by them. Article 28(1) seeks to ensure that controllers only engage processors who put in place sufficient guarantees for the security of personal data. Article 28(3) mandates a specific contract to be put in place between the controller and processor, which requires them to consider the nature and purpose of processing in order that those aspects of their relationship can be accurately reflected in the contract.[28] The contract also sets out how the relationship between a controller and processor should operate in practice,[29] and binds a processor to put appropriate security measures in place for the risk to personal data.[30]

9.26. The nature of SCU's infringement of Article 28 involved a failure to ensure that the Processor provided sufficient guarantees for the processing of personal data. SCU also failed to put in place a contract with the Processor that met the requirements of Article 28(3) of the GDPR.

9.27. In those circumstances, while there was a failure by SCU to adhere to that provision of the GDPR in respect of the Processor, which contributed to the Personal Data Breach, the underlying risk to rights and freedoms of data subjects caused by those infringements has been identified as being primarily due to the infringement of Articles 5(1)(f) and 32(1). Thus, the gravity of this infringement is light to moderate.

b) the intentional or negligent character of the infringement;

9.28. The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (the "**Fines Guidelines**") 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."*[31]

9.29. I recognise that SCU's infringements of the GDPR were not intentional nor deliberate acts or omissions. I therefore do not consider there was "intent" on the part of SCU in the sense that there was no knowledge or wilfulness on their part in respect of their failures to ensure compliance with the relevant provisions of the GDPR.

9.30. In the Fines Guidelines, the following examples and guidance are given in relation to negligence,

> *Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply*

[28] Article 28(3) of the GDPR

[29] Including Articles 28(3)(a), 28(3)(e), 28(3)(f), 28(3)(g) and 28(3)(h)

[30] Article 28(3)(c) of the GDPR.

[31] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679' WP253, 11

technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.

Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources.[32]

9.31. On this basis, I find that SCU was negligent within the meaning of Article 83(2)(b) in respect of the infringements identified in this Decision. While SCU is a small, community-based organisation, it was aware that it had obligations in relation to the processing of personal data under the GDPR, and failed to identify all of its processing operations, or to ensure that they were carried out in a manner that complied with that Regulation.

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

Articles 5(1)(f) and 32(1)

9.32. Following the Personal Data Breach, SCU took a significant number of steps to mitigate any damage that may have been suffered by data subjects. The Manager notified the Processor of the Personal Data Breach immediately on becoming aware of it. The next day, 30 November 2018, the Manager notified the Personal Data Breach to the DPC. By that time the Processor had taken a number of steps, described in the Breach Notification, including the following:

a) Access to the reports was immediately locked;

b) Google was requested to remove all affected records;

c) Director login passwords were changed;

d) www.slanecreditunion.ie was taken offline as a precaution;

e) A consultancy (the "**Consultancy**") was engaged to review the issue with the plugin and other security measures applicable to the website; and

f) SCU were carrying out an ongoing review of the accounts of each of the affected persons to confirm that all activity was validly authorised.

9.33. SCU provided the DPC with a screenshot of a www.google.com page removal confirmation relating to 13 links on 29 November 2018. On 4 November 2021, SCU confirmed that this request was made to Google to remove "any risk of links or search keywords being effective" to find the links.

9.34. SCU confirmed that all affected data subjects had been notified of the Personal Data Breach on 6 December 2018, six days after they became aware of the breach. Each data subject was also sent a separate letter providing them with a new SCU account number; this was described in the Breach Notification as one of the steps that SCU proposed to take to address the breach or mitigate its adverse effects.

[32] Ibid, 12

9.35. By 10 January 2019, SCU had received a list of recommended next steps from the Consultancy, and communicated to the DPC the steps that had been taken by SCU in response to those recommendations.

9.36. SCU compiled an incident report relating to the breach by 10 January 2019, and confirmed on 17 January 2019 that raw files relating to the Personal Data Breach had been saved. Those files have been provided to the DPC.

9.37. Over the next 16 months, at which point SCU sent their final submissions to the Inquiry Team on 22 May 2020, SCU took a number of steps to change the manner in which they processed member personal data in board reports. SCU reduced the timeframe for which directors' reports were stored from three years to three months, they removed old board packs, upgraded the board pack storage, and introduced download tracking for board packs. Subsequently, the Directors' Area was made redundant and board documents were shared with directors by unencrypted email or via SCU's secure website. By 13 March 2020, SCU had reduced the amount of personal data included in board packs. Instead of the information that had previously been included in the Member Enquiry Reports, SCU instead began to provide to directors the number of new members for the month and their account numbers, with more information available on request. On 22 May 2020, they said that information about new members was only provided in hard copy at board meetings and disposed of by directors securely, after the meeting.

9.38. In relation to the website more generally, SCU began to carry out documented website checks on a weekly basis. They put a change management policy in place on 12 July 2019.[33] They also submitted that the architecture of the website was changed to remove the use of plugins so that upgrades could not have the consequence that SCU identified as being attributable to the Yoast plugin in the context of the Personal Data Breach. They said that issues caused by outdated plugins and the content management system were identified by security checks, plugin checks and content management system checks; all plugins and systems were updated; and the website was transferred to a new server. They removed the Yoast plugin as a security measure for private files, but it was still enabled to serve its purpose of search engine optimisation. They further said that they made sure that private files were protected by measures like .htaccess and robots.txt instead of plugins.

9.39. On 25 April 2019, a website penetration test report was provided to SCU. The purpose of the test was to simulate an external attack on SCU's network and network services to identify any weaknesses that could be exploited by a non-approved person or entity.[34] The report identified a medium risk arising from one issue on the www.slanecreditunion.ie website, which involved an out of date version of PHP being used on the website.[35] An attempt to inject code into the director login page was blocked by a Wordpress security feature.[36]

[33] Final Inquiry Report, [45]
[34] Website penetration test 25 April 2019, [5]
[35] Ibid, [6]
[36] Ibid, [11]

9.40. In its submissions on the Draft Decision, SCU provided a copy of a risk assessment related to data protection from January 2022, the purpose of which was "to consider the risks to the processing of member personal data in director board packs and the security measures that are appropriate in respect of these risks." It specifies that member personal data is no longer included in board packs.[37]

Article 28

9.41. In relation to the infringement of Article 28, the Processor and the Sub-Processor are no longer engaged in data collection.[38] This is a mitigating action in relation to those infringements.

Articles 30(1)

9.42. In respect of the infringements of Article 30(1), an updated data inventory was provided to the DPC on 21 January 2022, which confirms that member personal data is not included in board packs.

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;

9.43. As outlined above, SCU infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures regarding its processing of Member Personal Data on the Directors' Area. I consider that SCU holds full responsibility for these failures and the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(f) and 32(1) against SCU, this factor cannot be considered aggravating in respect of those infringements.

9.44. In relation to the infringements of Articles 28 and 30(1), SCU put in place technical and organisational measures to ensure compliance with those provisions in some contexts. In relation to Articles 30(1) it adopted a data inventory on 21 May 2018. It updated some processor contracts to bring them in line with the requirements of Article 28(3). However, those technical and organisational measures did not fully capture the processing of Member Personal Data by SCU on the www.slanecreditunion.ie website during the Temporal Scope.

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

9.45. There are no relevant previous infringements of the GDPR by SCU.

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

9.46. SCU cooperated fully with the Inquiry Team throughout the Inquiry and sought to mitigate the infringements in the manner already described in this Decision. They responded to the queries circulated to them, and facilitated an onsite inspection of their premises. On 4

[37] On the fifth page of the January 2022 Risk Assessment

[38] SCU submissions of 22 May 2020, [44] and Data Processor Statement of Compliance with GDPR circulated on 21 January 2022

November 2021, they also responded to the request I sent them for further information on 14 October 2021.

9.47. I have had regard to the suite of documentation submitted by SCU with its submissions on the Draft Decision, and those submitted throughout the Inquiry, as detailed in the Appendix to this Decision. I find that SCU has shown a high degree of cooperation with the DPC and have taken many steps to remedy the infringements identified in this Decision and to mitigate their adverse effects.

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

9.48. Personal data of a financial nature was not affected by the infringement, and nor were any special categories of personal data. While Member Personal Data were processed by SCU for purposes that may have revealed their politically exposed status or criminal record,[39] the information in the Member Enquiry Reports did not in themselves contain special category data or data relating to criminal convictions or offences. Personal data of children were affected by the infringements, however.

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>

9.49. The Inquiry was conducted to examine whether or not SCU has discharged its obligations in connection with the subject matter of the Personal Data Breach and to determine whether any provision(s) of the GDPR or 2018 Act had been contravened by SCU in that context. Hence, SCU's notification of the Personal Data Breach triggered the process by which the infringements became known to the DPC.

9.50. 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."*[40]

9.51. Therefore, SCU's compliance with its obligation to notify personal data breaches under Article 33(1) of the GDPR cannot be considered mitigating in respect of the infringements of the GDPR identified in this Decision.

i) <u>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;</u>

9.52. Corrective powers have not previously been ordered against SCU with regard to the subject-matter of this Decision. I note that a previous inspection of certain features of SCU's website was carried out in 2016. As that investigation pre-dated the date of application of

[39] Submissions of 22 May 2020

[40] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, WP253, 15

the GDPR it is not a relevant aggravating or mitigating measure in respect of the application of any corrective measures in this Inquiry.

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

9.53. Not applicable.

k) <u>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.</u>

9.54. 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.

<u>Conclusion on the application of these criteria to the infringements by SCU</u>

9.55. 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)."*[41]

9.56. The Draft Decision proposed to impose an administrative fine in respect of SCU's infringements of Articles 5(1)(f), and 32(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 provide an effective, proportionate and dissuasive response in the particular circumstances of this case. In its submissions on the Draft Decision, SCU said,

> *In concluding our response, we are grateful to the Data Protection Commissioner for her observance and recognition of efforts done at the time and during the investigation. We have sought to meet the requirements intended for us prior to the finalisation of the report to show our determination in resolving any weaknesses and failures that have been identified.*
>
> *We sincerely hope that these additional measures will be recognised in the final report. Further, the Board respectfully states that, while it recognises that you may impose a maximum fine of €6,000, however it hopes that you look upon us favorably in this matter.*[42]

9.57. In deciding whether an administrative fine is appropriate in the circumstances and the amount of that fine, I have taken into consideration the additional steps taken by SCU to comply with the GDPR, as outlined in relation to the analysis of Articles 83(2)(c) and 83(2)(f)

[41] Ibid, 6.

[42] Document titled "Response to the Findings of the Data Protection Commissioner" circulated on 21 January 2022

of the GDPR above. I have also decided not to make an order to bring processing into compliance with the GDPR due to those additional steps taken by SCU, as previously outlined.

9.58. Regarding SCU's infringements of Articles 5(1)(f) and 32(1), while I consider that the reprimand is of significant value in dissuading future non-compliance and in re-establishing compliance with these provisions of the GDPR, the risk to the rights and freedoms of data subjects arising from the infringements warrants a fine in all the circumstances.

9.59. Regarding SCU's infringement of Article 30(1), I have taken account of the fact that the gravity of this infringement was considered to be light, and that it was considered not to be intentional.

9.60. In relation to the infringement of Article 28, this infringement presented a light to moderate risk to the rights and freedoms of data subjects. However, SCU had updated a number of processor agreements. It also mitigated the risk arising from this breach by halting its engagement of the processor in relation to the collection and processing of member personal data in board packs.

9.61. As a general comment, I note that SCU has been prompt to react following the Personal Data Breach, has been very cooperative with the DPC and has indicated a willingness to adopt any measures necessary to bring its processing into compliance with the GDPR.

9.62. However, for the reasons outlined above, I consider that an administrative fine is necessary, on balance, in order to ensure an effective, proportionate and dissuasive response to the infringements identified in respect of Articles 5(1)(f) and 32(1) of the GDPR. Accordingly, I have decided to impose a fine of €5,000 for the reasons explained in further detail below.

9.63. The findings of infringements of Articles 5(1)(f) and 32(1) relate to the processing by SCU of Member Personal Data in the Directors' Area. Article 32(1) elaborates on the requirement for appropriate security in Article 5(1)(f). In the circumstances, the infringements of Articles 5(1)(f) and 32(1) arise from the same failure of SCU to implement an appropriate level of security. Therefore, it is appropriate to calculate and apply a single administrative fine, and the fine will be calculated by reference to the infringement of Article 5(1)(f) only.

ii. The applicable range for the administrative fine

9.64. In determining the appropriate amount of an administrative fine, it is necessary to first identify 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 on that permitted range.

9.65. Article 83(5) of the GDPR provides that infringements of the obligations of controllers pursuant to, amongst others, Article 5 shall:

> *"…in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher…"*

9.66. The turnover of SCU in 2021 was €102,085.[43] As regards the maximum amount for the fine in respect of an infringement of Article 5(1)(f) is the higher of €20,000,000 or 4% of the turnover for the preceding financial year. Therefore, I am satisfied that the cap for SCU's infringement of Article 5(1)(f) is €20,000,000. This cap is not a starting point, but rather the cap on the permitted range as provided for by Article 83(5) of the GDPR.

iii. Calculating administrative fine

9.67. In the absence of specific EU-level guidelines on the calculation of fines, I am not bound to apply any particular methodology.[44] 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 SCU, as the addressee, to understand the basis for the fine and ensuring that the fine is calculated in a rational manner.

9.68. The first step in the methodology I have followed in calculating the 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(5) of the GDPR is not the starting point. Rather, it is relevant to determining the permitted range. The determination of where on the permitted range the appropriate proposed range lies is made by reference to the nature, gravity, and duration of each infringement, as considered in relation to Article 83(2)(a) above, and the other mitigating and 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. Then it will be considered whether the figure arrived at is "*effective, proportionate and dissuasive*" in the circumstances in accordance with Article 83(1) of the GDPR.

9.69. 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 SCU with the opportunity to comment in accordance with fair procedures. In its submissions on the Draft Decision, SCU made the comments outlined at paragraph 9.56, highlighting the additional steps it had taken and asking the DPC to look upon it favourably. As noted above, I have taken those submissions into consideration in relation to the application of the criteria set out in Article 83(2)(a)-(k) of the GDPR. In particular, I consider these steps to be mitigating in line with Article 83(2)(c) and 83(2)(f) of the GDPR.

9.70. In locating the fine on the permitted range of €0 to €20,000,000, 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 infringements as assessed in accordance with Article 83(2)(b) above. I have also had regard to the mitigating factors outlined in accordance with Articles 83(2)(c) and 83(2)(f) and have had regard to SCU's submissions in that respect.

[43] The figure listed beside "Total Income for Year" in SCU's audited financial statements for the year ended 30 September 2021, submitted by SCU to the DPC along with its submissions on the Draft Decision on 21 January 2022.

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

9.71. Based on the analysis above, I find that the final figure for the administrative fine in this Decision in respect of SCU's infringement of Article 5(1)(f) of the GDPR is €5,000.

9.72. 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 €5,000 meets these requirements. As outlined above, the outlined infringement creates risks to the rights and freedoms of data subjects. In order for a fine to be dissuasive, it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. I am satisfied that the final figure would be dissuasive to both SCU and similar controllers. As regards the requirements 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 fine outlined 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.

10. Summary of corrective powers

10.1. By way of summary, this Decision has imposed the following corrective action:

- A reprimand; and
- An administrative fine of €5,000.

11. Right of Appeal

11.1. This Decision is issued in accordance with Section 111 of the 2018 Act. Pursuant to Section 150(5) of the 2018 Act, SCU 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, SCU 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.

_____

Helen Dixon

Commissioner for Data Protection

Appendix: Schedule of materials considered for the purposes of this Decision

1. Draft Inquiry Report
2. Final Inquiry Report
3. Appendices D.1 to D.9 to Final Inquiry Report:
    - D.1. Breach Notification File
    - D.2. Commencement Letter 19 July 2019
    - D.3. Slane Credit Union Replies to Commencement Letter
    - D.4. Slane Credit Union Submissions December 2019
    - D.5. DPC correspondence 5 March 2020
    - D.6. Slane Credit Union Submissions 13 March 2020
    - D.7. Slane Credit Union Submissions to the draft Inquiry Report 22 May 2020
    - D.8. Yoast Website snapshot 28 July 2020
    - D.9. Clarification of submission
4. Slane Credit Union Submissions 4 November 2021
5. Slane Credit Union Submissions on the Draft Decision, titled "Response to the Findings of the Data Protection Commission" dated 21 January 2022 and the following enclosed documents:
    - 5.1. Slane Credit Union Data Protection GDPR Policy
    - 5.2. Slane Credit Union Data Inventory
    - 5.3. Data Processor Statement of Compliance with GDPR
    - 5.4. Slane Credit Union Risk Assessment related to Data Protection January 2022
    - 5.5. Service provider agreements and correspondence
    - 5.6. Slane Credit Union Financial Statements 30 September 2021