In the matter of the General Data Protection Regulation

Commission Case Reference: IN-21-2-1

In the matter of Allianz plc

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

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

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

28 June 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. Introduction

1. This document is a decision (the **'Decision'** or the **'Final Decision'**) made by the Data Protection Commission (**'the Commission'**) in accordance with section 111 of the Data Protection Act 2018 (**'the 2018 Act'**). I make this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act.

2. Allianz was provided with the draft decision in this Inquiry on 1 June 2022 (the **'Draft Decision'**) to provide it with a final opportunity to make submissions. This Decision is being provided to Allianz pursuant to Section 116(1)(a) of the 2018 Act in order to give Allianz notice of the Decision and the reasons for it.

B. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

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

4. Section 110(1) of the 2018 Act provides that the Commission 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 2018 Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the Commission may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

b) Data Controller

5. In commencing the Inquiry, the Commission considered that Allianz may be the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that were the subject of personal data breach notifications made by Allianz to the Commission. In this regard, Allianz confirmed that it was the controller in its notification of the personal data breaches to the Commission between 25 June 2020[1] and 31 December 2020.[2]

[1] Note: Breach Notifications BN-20-7-36, 68 and 88 were reported in June 2020 but assigned July 2020 reference numbers by the Commission

[2] Appendix C.2 Breach Notifications

c) Legal Basis for the Decision

6. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the Commission 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 as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the Commission. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry and any other materials which I consider to be relevant, in the course of the decision-making process.

7. An Inquiry Issues Paper was issued by the Commission to Allianz on 27 July 2021. Allianz provided submissions on the Inquiry Issues Paper on 31 August 2021.

8. Having considered the information obtained in the Inquiry, I am satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. The Draft Decision was provided to Allianz on 1 June 2022 and Allianz was provided with an opportunity to make submissions on the Draft Decision. In a letter dated 22 June 2022, Allianz stated that after having considering the Draft Decision, Allianz had no further submissions to make in respect of the Inquiry.

C. Factual Background

9. Allianz notified the Commission of forty-nine personal data breaches between 25 June 2020[3] and 31 December 2020. Of the data breaches, 35 were postal disclosures, 13 were email disclosures, while one was other human error. Allianz identified that out of 48 of those 49 personal data breaches, 60 data subjects were directly affected. For the remaining data breach (BN-20-10-437) Allianz was unable to quantify the number of affected data subjects affected when a letter about the policy was sent to the wrong recipient.

10. The Commission issued an Inquiry Commencement Letter (‘**the Commencement Letter’**) by email and registered post to Allianz on 23 February 2021[4] notifying the organisation that the Commission had commenced an Inquiry under and in accordance with Section 110(1) of the 2018 Act. The letter contained details of the personal data breaches notified to the Commission which would be the subject of the Inquiry and contained seven questions seeking further information from Allianz.

11. The decision to commence the Inquiry was taken having regard to the circumstances of the personal data breaches notified by Allianz. The Commencement Letter informed Allianz that the Inquiry would examine whether or not Allianz discharged its obligations in connection with the subject matter of the personal data breaches and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by Allianz in that context.

12. The Commencement Letter set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The relevant facts ascertained during the personal data breach

[3] Note: Breach Notifications BN-20-7-36, 68 and 88 were reported in June 2020 but assigned July 2020 reference numbers by the Commission

[4] Appendix C.3 Commencement Letter

notifications and handling process were set out in the Commencement Letter. The facts, as established during the course of the Inquiry, are set out below in this Decision.

13. Allianz provided submissions in response to the Commencement Letter on 31 March 2021.[5] In its submissions, Allianz outlined the technical and organisational measures which Allianz had in place to meet the requirements of the GDPR. The submissions outlined policies and procedures in relation to data protection governance.

14. The submissions also outlined the steps that Allianz has taken since the personal data breaches occurred in order to comply with the GDPR. The submissions appended a number of documents, which are considered throughout this Decision.

15. On 26 April 2021,[6] the Case Officer requested additional information in relation to some of the data breaches. Allianz provided submissions in response on 11 May 2021.[7]

16. Having received and examined Allianz's submissions, the Commission prepared an Inquiry Issues Paper to document the relevant facts provisionally established and the issues that fell for consideration by me as decision maker for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry. The Case Officer furnished Allianz with the Inquiry Issues Paper on 27 July 2021[8] and invited Allianz's submissions on any inaccuracies and/or incompleteness in the facts.

17. Allianz provided submissions on the Inquiry Issues Paper on 31 August 2021.[9] The comments included some textual amendments and supplemental information relating to the facts as set out in the Inquiry Issues Paper. Those comments were analysed and the Commission has considered them as part of this Decision.

18. I am obliged to consider all of the information obtained in the Inquiry and to reach conclusions as to whether I identify infringements of data protection legislation and if so whether corrective powers should be exercised. The matters set out in this document are subject to change, as might be required to take account of any submissions that might be made by Allianz.

D. Scope of the Inquiry

20. The scope of the Inquiry, which was set out in the Commencement Letter, was to examine whether or not Allianz discharged its obligations in connection with the subject matter of certain specified personal data breaches and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR have been contravened by Allianz in that context.

21. In this regard, the Commencement Letter specified that the Inquiry would focus on Allianz's organisational and technical measures in place to ensure security of the personal data.

22. The material scope of the GDPR under Article 2 applies to the processing of personal data. This Decision concerns data encompassing Allianz's customers' names, date of birth and in some cases

[5] Appendix C.4 Submissions 31 Mar 2021
[6] Appendix C.5 Queries 26 Apr 2021
[7] Appendix C.6 Submissions 11 May 2021
[8] Appendix C.7 Issues Paper
[9] Appendix C.8 Submissions 31 Aug 2021

policy documents. This meets the definition of personal data under Article 4(1) GDPR. The data was disclosed / accessed through processing by Allianz using its postal and email systems.

E. Issue for Determination: Compliance with Article 32(1)

23. Having reviewed the Inquiry Issues Paper and the other relevant materials, I consider the key issue in which I must make a Decision is whether Allianz has infringed Article 32(1) of the GDPR.

24. Article 32(1) of the GDPR provides:

> '*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.*'

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

i. Assessing Risk

26. The level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the processing. Article 32(2) of the GDPR expressly states that the risks of alteration or unauthorised disclosure should be considered when assessing the appropriate level of security.

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

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

28. Regarding the nature, scope, context and purposes of Allianz's processing of personal data, the nature of Allianz's processing is sensitive as communications contain contact details and relate to insurance policies of customers. Insurance documents can also process data relating to the health of data subjects which is a special category of personal data under Article 9 of the GDPR.

29. The scope of Allianz's processing of personal data is extensive. This is illustrated by the statistics Allianz provided. [redacted] The context and purpose of the processing of personal data is to enable Allianz to fulfil its contractual obligations to its customers. Considering the volume of personal data processed the risk of an unauthorised disclosure of personal data occurring is high.

30. The unauthorised disclosure of personal data could also result in material or non-material harm to data subjects of moderate severity. Emotional distress can be caused by the unauthorised disclosure of personal data. Trust between a customer and Allianz can be undermined if personal data is disclosed without a customer's authorisation. Personal data breaches undermine a data subject's reasonable expectation of privacy. In disclosing customers' contact details, addresses and names the exposure of data subjects' to identity theft is also increased. Due to the volume of the personal data being processed by Allianz I find the likelihood of the risk being realised is high.

31. Overall, I find the processing operations of Allianz which fall for consideration in this Decision pose a moderate risk to the rights and freedoms of individuals.

ii. Security measures implemented by Allianz

Policies and Procedures

32. Allianz outlined that it had introduced a range of policies and procedures in relation to data protection as part of the implementation of the GDPR. Its data protection governance structure, which, it stated, includes three lines of defence,[10] involving day to day management, assurance functions and, finally, Internal Audit. The Allianz Compliance Policy,[11] which was in place prior to the period of the breaches, describes the three lines of defence model in detail. It also sets out individual staff responsibilities, including in relation to confidentiality, security and accuracy of communications.

33. Allianz also stated that it has the following policies in place with regard to outbound electronic communications. These policies were provided with the Allianz submissions of 31 March 2021:[12]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[10] Appendix C.4.2 pages 8-9
[11] Appendix C4.4
[12] Appendix C.4

34. Allianz indicated that the email guidelines, which originally date from 2012, were under review in 2021 and due to be updated.

35. On 24 July 2020, Allianz put in place an External Email Warning Tool for all outbound external emails.[13] The tool was described as a prompt to the staff member to double check the external email address:

> *"This enables staff to clearly see the relevant email address."*

36. Allianz explained that it uses post for customers who do not use MyAllianz,[14] for issuing policy documents to intermediaries and for other ad-hoc purposes. Allianz outlined that the majority of its printing is automated.

37. According to Allianz, where manual printing is required, processes are in place to ensure that policies are followed, including weekly spot checks to ensure that documents have been correctly addressed. Allianz stated that it has *"implemented daily cross/spot checks instead. These checks are now recorded which was not the case with the weekly cross/spot checks."*[15]

Training and Awareness

38. Allianz provided details of its training, education and awareness programmes for staff, which includes: new starter induction training; annual data protection training; specific business area training; and intranet training.

39. Allianz provided a number of training related documents with its submissions of 31 March 2021. Both the *Data Protection in Allianz (2020)*[16] and the *Data Privacy and GDPR in Allianz (2020)*[17] are data protection specific training modules. Allianz also provided a *Data Breach Blog*,[18] which is available for staff via the intranet. Allianz also described how it was in the process of implementing a '*Privacy Champions*' project, which was due for completion in 2021.

40. Allianz stated that staff are trained to use the email 'reply' function when responding to inbound emails.

> *"This practice eliminates the identified risk of incorrect population of the email* address*. It is Allianz practice to only respond to the email once we have verified that the email is from a trusted customer. Allianz agents are trained to adopt and follow this practice."* [19]

41. Of the 49 personal data breaches under investigation that occurred between 25 June 2020[20] and 31 December 2020, 35 were postal disclosures. According to Allianz, all staff receive data protection training on an annual basis, including staff in the DST (the postroom) in January 2020 and in the Direct Business Area in July 2020.[21]

---

[13] Appendix C.4.2 page 18 at 1.5.8
[14] MyAllianz is an on-line self service portal, which allows customers to securely manage insurance policies
[15] Appendix C.6.2 page 4
[16] Appendix C.4.13
[17] Appendix C.4.14
[18] Appendix C.4.15
[19] Appendix C.4.2 page 11
[20] Note: Breach Notifications BN-20-7-36, 68 and 88 were reported in June 2020 but assigned July 2020 reference numbers by the Commission
[21] Appendix C.6.2 page 2

Records Management

42. Allianz outlined that it had a range of oversight measures in place for the processing of personal data through its email and postal systems. These include

- The Data Classification Security Policy[22] – this policy classifies documents as being 'public', 'internal', 'confidential' and 'strictly confidential and sets out whether such documents require encryption if being transmitted.
- The Data Classification Security Policy Cheat Sheet[23] is a quick reference guide provided to staff with regard to the above classifications.
- [redacted] – Allianz described that the tool is used

  "[redacted]

- Post room / DST measures and processes – Allianz outlined that the majority of its sorting and printing is done by fully automated processes. However, in cases where automation is not possible, Allianz indicated that it has manual procedures in place:

  "The DST separate printing and insertion into separate processes and also break them down further by product type to reduce the risk of mistakes. This means that all documents requiring the same insert are grouped together, thus mitigating the risk of sending out incorrect documents to customers."

Data Security Measures

43. [redacted]

44. Allianz described the security measures it has built in to the portal's functionality in order to minimise the risk of sending documentation to an incorrect recipient, including double-factor authentication.[25] Allianz also indicated that it is developing an eDocs facility with its intermediaries:

"This project will provide broker Intermediaries with direct access to policy documentation which they can then issue to customers with a reduced involvement from DST (i.e. DST will be required to print and

[22] Appendix C.4.18
[23] Appendix C.4.10
[24] Appendix C.4.2 pages 29
[25] Appendix C.4.2 pages 10-11

send policies to Intermediaries in reduced circumstances). This will reduce the volume of communications to be sent by us to Intermediaries. This, in turn, will reduce the likelihood of personal data breaches in this regard."[26]

45. Allianz listed its organisational measures in relation to data security, some of which have already been described. Allianz stated that it

> *"implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including by reviewing and updating such measures to augment and build upon the existing measures to reflect evolving best practices. These measures and our comprehensive data protection programme are documented in numerous data protection related policies and procedures, and are subject to an appropriate oversight functionality. This includes the following:*
>
> - *Specialist Data Protection Officer and Data Protection Function*
> - *Specialist Information Security Officer and Information Security Team*
> - *Data accuracy measures and processes*
> - *Electronic communications measures and processes*
> - *Post room / DST measures and processes*
> - *Measures with Intermediaries*
> - *Personal data breach policies and procedure*
> - *Information Security policies and procedure*
> - *Business continuity, disaster recovery and cyber security frameworks*
> - *Quality assurance programme*
> - *Compliance Function and Internal Audit Function*
> - *Training, education and awareness programme.*
> - *Ongoing review, testing and augmentation"*[27]

iii. Appropriate Security Measures

46. Considering the risks to data subjects associated with Allianz's processing operations, it is incumbent on Allianz to implement appropriate security measures to minimise the possibility of the risks materialising in accordance with Article 32(1).

47. Article 32(1) does not require Allianz to ensure that zero personal data breaches occur nor does it impose a strict liability standard on controllers where a personal data breach does occur. Rather the controller is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The required standard to be met by controllers is not a static concept and must be continuously re-evaluated in light of the risks posed. For example, the repetition and accumulation of personal data breaches in a particular segment of the business is indicative of an increased risk profile and the controller or processor is required to take steps to reduce this risk. In light of the personal data breaches that occurred in this case, Allianz ought to conduct a new risk assessment with the aim of preventing the reoccurrence of personal data breaches with similar root causes and to implement appropriate technical and organisational measures to achieve this.

[26] Appendix C.4.2 pages 29-30
[27] Appendix C.4.2 page 6

48. Overall, I find Allianz has not infringed Article 32(1) in this case. The security measures implemented by Allianz were appropriate with regard to risks associated with the processing. It is notable that although the breaches were variegated in nature, Allianz had specific policies which contained guidance on how to minimise these risks. For example, Allianz had clear guidelines for employees in place which emphasised the importance of verifying the address of recipients prior to sending emails and it had scripts for staff in call-centres to verify the accuracy of personal data submitted by customers. Allianz engaged in continuous re-evaluation of its data protection policies which is evidenced by the recent DP Privacy Champions initiative.

49. I also find that Allianz data protection training programmes met the requirements under Article 32(1). All staff received data protection training. Allianz also provided tailored data protection training to areas most susceptible to personal data breaches including DST and Direct Business.[28] This was evidenced by training invites dated 30 January 2020[29] and 15 July 2020.[30]

50. Allianz also demonstrated an awareness of the increasing risk profile of some areas of its business in terms of susceptibility to personal data breaches by implementing measures seeking to reduce the risk of reoccurrence. An example, of a measure implemented by Allianz was the External Email Warning Tool for all outbound external emails implemented on 24 July 2020. I find this was an appropriate security measure to implement in light of the increasing risk profile posed by the increased incidence of personal data breaches occurring on foot of incorrect email addresses being entered. The introduction of increased spot checks in the post room was also another appropriate security introduced to address an increasing risk profile associated with processing.

51. Moreover, while noting that the quantum of personal data breaches, in of itself, is not a basis for finding an infringement (or a lack of an infringement) of Article 32(1), the finding that Allianz has complied with Article 32(1) is underscored by the fact that the personal data breaches that occurred were relatively low when compared with the scale of Allianz's processing operations over this period. [redacted]

[redacted]

[28] Appendix D.4.2 Submissions 31 Mar 2021 page 45.
[29] Appendix D.5.6 Training Invite to DST January 2020
[30] Appendix D.5.5 DP Training to Direct July 2020.

52. Another relevant consideration is that the personal data breaches considered individually were not of a serious gravity nor did they affect a large number of data subjects. From 48 breach notifications, 60 data subjects were affected and in relation to one breach the number of data subjects affected could not be confirmed.

53. In conclusion, having taken into account, the state of the art, the costs of implementation of security measures and the nature, scope, context and purposes of Allianz's processing as well as the high likelihood and moderate severity of the risk for the rights and freedoms of natural persons, I find Allianz has implemented appropriate technical and organisational measures as required under Article 32(1) of the GDPR.

F. Right of Appeal

54. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, Allianz has the right to appeal against this Decision within 28 days from the date on which notice of this Decision is received by it.

_____

Helen Dixon

Commissioner for Data Protection