In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-6-1

In the matter of Ark Life Assurance Company dac

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

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

DECISION

Decision-Maker for the Data Protection Commission:

Helen Dixon
Commissioner for Data Protection

26 September 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. Ark Life was provided with the draft decision in this Inquiry on 18 August 2022 (the 'Draft Decision') to provide it with a final opportunity to make submissions. This Decision is being provided to Ark Life pursuant to Section 116(1)(a) of the 2018 Act in order to give Ark Life 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 DPC 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 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 2018 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.

b) Data Controller

5. In commencing the Inquiry, the DPC considered that Ark Life 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 Ark Life to the DPC. In this regard, Ark Life confirmed that it was the controller in its notification of the personal data breaches to the DPC.

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

7. An Inquiry Issues Paper was issued by the DPC to Ark Life on 29 April 2022. Ark Life provided submissions on the Inquiry Issues Paper on 20 May 2022.

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 Ark Life on 18 August 2022 and Ark Life was provided with an opportunity to make submissions on the Draft Decision. In a letter dated 2 September 2022, Ark Life provided submissions on the Draft Decision.

C. Factual Background

9. The DPC received 156[1] personal data breach notifications from Ark Life during the period December 2018 to May 2021. The data breaches primarily concerned the unauthorised disclosure of personal data as a result of address inaccuracies and issues within the postal and email procedures operated by Ark Life.

10. The DPC issued an Inquiry Commencement Letter ('**the Commencement Letter'**) by email and registered post to Ark Life on 8 June 2021[2] notifying the organisation that the DPC 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 DPC that would be the subject of the Inquiry and contained eight questions seeking further information from Ark Life.

11. The decision to commence the Inquiry was taken having regard to the circumstances of the personal data breaches notified by Ark Life. The Commencement Letter informed Ark Life that the Inquiry would examine whether or not Ark Life 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 Ark Life 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 notifications and handling process were set out in the Commencement Letter. The facts, as provisionally established during the course of the Inquiry, are set out below in this Decision.

13. Ark Life provided submissions in response to the Commencement Letter on 6 July 2021.[3] In its submissions, Ark Life outlined the technical and organisational measures that Ark Life 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 Ark Life 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. Having received and examined Ark Life's submissions, the DPC prepared an Inquiry Issues Paper to document the relevant facts provisionally established and the issues that fell for consideration

[1] Appendix C.1 – BN Classifications - Final
[2] Appendix C.2 – Commencement Letter
[3] Appendix C.3 – Submissions 6 July 2021

by me as decision maker for the purpose of making a decision under section 111 of the 2018 Act in respect of this Inquiry.

16. The Case Officer furnished Ark Life with the Inquiry Issues Paper on 29 April 2022[4] and invited Ark Life's submissions on any inaccuracies and/or incompleteness in the facts. Ark Life provided submissions on the Inquiry Issues Paper on 20 May 2022.[5] The comments included some textual amendments and supplemental information relating to the facts as set out in the Inquiry Issues Paper.

17. On 2 June 2022 the Case Officer requested additional information in relation to some of the data breaches. Ark Life provided submissions in response on 16 June 2022.[6] Those submissions were analysed and the DPC has considered them as part of this Decision.

18. Ark Life was provided with the Draft Decision on 18 August 2022. Ark Life provided submissions on the Draft Decision on 2 September 2022.[7] The comments included some textual amendments and supplemental information relating to the facts as set out in the Draft Decision. Those comments were analysed and the Commission has considered them as part of this Decision.

19. 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.

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 Ark Life 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 Ark Life in that context.

20. In this regard, the Commencement Letter specified that the Inquiry would focus on Ark Life's organisational and technical measures that are in place to ensure security and accuracy of the personal data involved, particularly in relation to its postal and email processes. The Inquiry would also examine associated policies and procedures that are in place that identify any risk to data subjects and the organisational and technical measures to address those risks.

21. The material scope of the GDPR under Article 2 applies to the processing of personal data. This Decision concerns data encompassing Ark Life's customers' names, date of birth and in some cases policy documents. This meets the definition of personal data under Article 4(1) GDPR. The data was disclosed / accessed through processing by Ark Life using its postal and email systems.

[4] Appendix C.6 Issues Paper
[5] Appendix C.4 Submissions 20 May 2022
[6] Appendix C.5 Submissions 16 June 2022
[7] Appendix C.7 Submissions 2 September 2022

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

22. 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 Ark Life has infringed Article 32(1) GDPR.

23. Article 32(1) 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.*'

24. In considering the technical and organisational measures that are appropriate for a controller or processor to 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

25. 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) GDPR expressly states that the risks of alteration or unauthorised disclosure should be considered when assessing the appropriate level of security.

26. 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."*

27. Regarding the nature, scope, context and purposes of Ark Life's processing of personal data, the nature of Ark Life's processing is sensitive as communications contain contact details and relate to life assurance policies of customers. Life Assurance documents can also contain data relating to the health of data subjects, which is a special category of personal data under Article 9 GDPR.

28. The scope of Ark Life's processing of personal data is extensive. In its response to the Commencement letter Ark Life stated that it issues approximately 200,000 outbound customer communications annually. Ark Life's products are typically long-term where customers may not contact Ark Life for a number of years at a time. This presents an additional challenge vis-á-vis maintaining up to date contact details for customers. The context and purpose of the processing

of personal data is to enable Ark Life 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.

29. The unauthorised disclosure of personal data could also result in material or non-material harm to data subjects of moderate severity to low severity, depending upon the nature of the correspondence. Emotional distress can be caused by the unauthorised disclosure of personal data. Trust between a customer and Ark Life 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, address and names the exposure of data subjects' to identity theft is also increased. Due to the volume and nature of the personal data being processed by Ark Life I provisionally find the likelihood of the risk being realised is high, but the severity of the impact is moderate to low.

ii. Security measures implemented by Ark Life

Policies and Procedures

30. Ark Life initiated a formal GDPR Programme in 2017 to assess and address risks pertaining to the new GDPR requirements. Among the main risks and appropriate actions identified in this project were:

    - Renew and update existing outsourcing agreement with its Outsource Service Provider ('**OSP**'), Irish Life Financial Services
    - Renew Ark Life Privacy Notice
    - Procedure and process documents were reviewed for data breach notifications, data subject, access requests and DPIAs
    - A record of processing activities for each area was created
    - Employee privacy notice and Data subject access request procedures were reviewed[8]
    - Data retention policy drafted

31. A Risk and Compliance Sub-Committee and Board Risk Committee was set up to provide second line reporting and, according to Ark Life, both of these were in existence prior to 2017.[9] A monthly governance forum was established to keep up to date with reported data breaches and to track required measures to mitigate against further risks. As of August 2021, '*Personal Data breaches and further measures*' is a standing agenda item. Internal Audit completed the '*3 lines of defence*' reporting model.

32. Between 2019 and 2021, regular Internal Compliance Monitoring reviews identified further inherent issues with the Address Update and Returned Mail processes and issues relating to adherence to these processes, namely the application of **correspondence holds** and maintaining **up to date details for customers**. This necessitated the implementation of a number of system and process changes. It also prompted Ark Life to review historic cases. This review was completed in July 2021.

[9] Appendix C.7 DPC Response Submission Letter 2 Sept 2022

33. Ark Life has a monthly Key Risk Indicator (KRI) to track the volume of personal data breaches.

Training and Awareness

34. Ark Life introduced compulsory Data Protection training as part of its GDPR Programme in 2018 to address GDPR knowledge gaps. An extract of the training resource was provided in its submissions of 6 July 2021. All employees must complete this training annually with a pass rate of 85%.

35. Enhanced training was delivered between February and August 2019 updated to include the issues with its Address Update and Returned Mail procedures referred to above.

36. Refresher training on Data Protection Breach Awareness and Prevention was delivered in September 2021. This training was tailored to address the identified root causes of the breaches reported in this inquiry and was extended to all customer service teams involved with outbound correspondences.

37. Ark Life conducted a workshop with its OSP Customer Service Management in September 2021 to outline to Managers the required training to be given to its teams.

Oversight Measures

38. Ark Life outlined that it had a number of oversight measures in place for the processing of personal data through its email and postal systems namely 'Address Update' and 'Returned Mail' procedures.

39. Correspondence holds were to be applied to accounts in the event of returned mail. This procedure underwent a number of corrective changes in response to the discovery of inherent issues in the process.

    - In March 2018, prior to the scope of this inquiry, this process was hardened to correct an issue whereby correspondence holds were not being applied to business customers.
    - In March 2020 a further change was implemented to prevent Annual Benefit Statements being issued to customers for whom a correspondence hold had been applied.
    - In March 2021 a further change was completed to isolate cases of returned post where a hold had not been applied and system check to confirm if one still required.

40. A review of historic cases was completed in July 2021.

41. A workshop conducted with the OSP Customer Service Management in September 2021 did not identify any further sources of errors arising from the application of correspondence holds.

42. Staff were instructed to ask customers to confirm contact details during inbound calls. Quality checks were undertaken to confirm adherence.

43. Ark Life has operated a 'closed book' of business since 2012. This and the long-term nature of its services mean that inbound communication from customers is of a sporadic nature. As a result Ark Life implemented a number of initiatives to maintain correct contact details for its customers.

    - A former associated agent of Ark Life implemented a process known as the 'Nightly Feed'. If a customer of this agent who also holds a plan with Ark Life, changes his/her address in one of their branches, staff ask for consent to notify Ark Life of a change of address.
    - The Annual Benefit Statement sent to each personal pension customer also contained and address update reminder prompting them to inform Ark Life of any address changes.
    - The former associated agent issued write out campaigns on behalf of Ark Life. Quality checking procedures were put in place to test adherence to the Nightly Feed and Address Update procedures.

iii. Appropriate Security Measures

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

45. Article 32(1) does not require Ark Life 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, Ark Life 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.

46. The security measures implemented by Ark Life were appropriate with regard to risks associated with the processing. It is notable that although the breaches were of various natures, Ark Life had specific policies which contained guidance on how to minimise these risks. For example, Ark Life had clear guidelines for employees in place which emphasised the importance of verifying the address of recipients prior to sending emails and procedures in place to prevent correspondences being issued when a hold was in place. Ark Life engaged in continuous re-evaluation of these

procedures by means of checking historic cases, identifying root causes and implementing system and process changes accordingly.

47. I also find that Ark Life data protection training programmes met the requirements under Article 32(1). All staff must undergo data protection training. Ark Life also provided enhanced data protection training to areas most susceptible to personal data breaches and this training was continuously tailored to incorporate the issues and process changes outlined above. Ark Life 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. Examples of these are the system changes to its existing processes summarised in paragraphs 40 to 44 above.

48. I note 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 provisional finding that Ark Life has complied with Article 32(1) is underscored by the fact that the number of personal data breaches that occurred was relatively low when compared with the scale of Ark Life's processing operations over this period. Between 25 May 2018 and 8 June 2021 Ark Life issued approximately 600,000 outbound communications. The number of reported personal data breaches relative to this number is less than 0.03% of those communications. Furthermore, Ark Life has demonstrated that since the end of the temporal scope of this inquiry to the present day, the implemented measures have brought about a further reduction in the rate of breaches.

49. 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 Ark Life's processing as well as the high likelihood and moderate to low severity of the risk for the rights and freedoms of natural persons, I provisionally find Ark Life has implemented appropriate technical and organisational measures as required under Article 32(1) GDPR. Overall, I provisionally find Ark Life has not infringed Article 32(1) in this case.

F. Right of Appeal

50. The final Decision will issue in accordance with section 111 of the 2018 Act. Section 150(5) gives a person affected by a legally binding decision of the DPC a right of appeal within 28 days from the date on which notice of this Decision is received by it.