idpc. INFORMATION AND DATA PROTECTION COMMISSIONER

Information and Data Protection Commissioner

CDP/COMP/193/2025

Ramon Mangion

vs

LifeStar Insurance plc

COMPLAINT

1. On the 11th April 2025, [redacted] (the **"complainant"**) lodged a data protection complaint with the Information and Data Protection Commissioner (the **"Commissioner"**) pursuant to article 77(1) of the General Data Protection Regulation[1] (the **"Regulation"**), alleging that [redacted][2] (the **"insurance company"**) had infringed the provisions of the Regulation.

[redacted]

FACTS OF THE CASE

2. For the purpose of this complaint, the Commissioner assessed the relevant facts as follows:

   i. that that the insurance company had once again permitted a third-party to contact him in relation to its insurance products, notwithstanding the Commissioner's previous decision of the 4th October 2024[3], which had clearly established that no representative or intermediary acting on behalf of the insurance company was to make any further contact with him;

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[redacted] (according to the Malta Business Registry records accessed on the 4th May 2026).

[3] Commissioner's decision, [redacted]

ii. that upon receiving the call from [redacted] (the **"third-party company"**), he immediately informed the caller that the matter had already been investigated and definitively decided by the Commissioner, following which the caller apologised and indicated that the issue would be verified internally; and

iii. that the insurance company had failed to update its systems in accordance with the Commissioner's decision, as his telephone number continued to be shared for marketing purposes and was not excluded from call lists, thereby infringing his rights under data protection law.

INVESTIGATION

Request for Submissions

3. Pursuant to the internal investigative procedure of this Office, the Commissioner sent a copy of the complaint, including the supporting documentation, and provided the insurance company with the opportunity to make any submissions which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

[redacted]

Submissions made by the insurance company

4. On the 30th April 2025, the insurance company submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:

i. that two (2) outbound calls were placed to the complainant on the 4th April 2025 in contravention of the Commissioner's decision of the 4th October 2024[4];

ii. that the cause was identified as a one-off internal deletion of seven (7) rows from the insurance company's interim *'Do-Not-Call'* spreadsheet, which suppressed the flag that would have blocked the dialler;

[4] Ibid.

iii. that outbound activity by the marketing agent was halted immediately, the master *'Do-Not-Call'* list was restored and redistributed the same day and a fully automated suppression mechanism is scheduled to go live by the end of Q3 2025;

iv. that the insurance company provided an explanation of the chronology of events;

Date	**Event**
27th February 2023	The complainant lodged a complaint[5] with the Commissioner after sending two (2) emails to the insurance company, dated the 26th and the 31st January 2023, in which he exercised his rights under article 15, article 17 and article 21(3) of the Regulation, without receiving any reply.
28th March 2023	The insurance company informed the complainant that his number would be removed from its systems. An interim single *'Do-Not-Call'* spreadsheet was adopted and the Commissioner subsequently closed the case.
11th June 2024	The complainant received a cold call from a Key Business Introducer of the insurance company and filed another complaint[6].
24th June 2024	The Commissioner informed the insurance company of this complaint.
9th August 2024	The insurance company explained that the call was generated by a random sequence of digits and that the caller had overlooked the *'Do-Not-Call'* list.
4th October 2024	The Commissioner issued a decision[7], finding an infringement of article 21(2) of the Regulation.

[5] Complaint received on the 27th February 2023, and registered internally as [redacted]
[6] Complaint received on the 11th June 2024, and registered internally a[redacted]
[7] Ibid 3.

March 2025	A new Key Business Introducer was onboarded and provided with the *'Do-Not-Call'* list.
4th April 2025 *(at 9.46am and 10.06am)*	The two (2) calls were placed to the complainant by the new Key Business Introducer's call centre.
11th April 2025	The complainant submitted a further complaint to the Commissioner[8], alleging infringement of article 21(2) of the Regulation.
17th April 2025	The insurance company was duly notified of this complaint by the Commissioner.
22nd April 2024	An internal investigation revealed that the first seven (7) rows of the *'Do-Not-Call'* list, including the complainant's mobile number, had been inadvertently deleted during the export to the new Key Business Introducer, resulting in a suppression failure.

v. that the calls of the 4th April 2025 were not the result of deliberate marketing to known customers but flowed from a single error that stripped the record from the suppression list. No other personal data concerning the complainant is processed by the insurance company beyond the suppressed number and correspondence file;

vi. that the outbound activity by the Key Business Introducer was suspended until acknowledgment of the corrected list, following which the full *'Do-Not-Call'* list was restored and redistributed to all Key Business Introducers;

vii. that an automated suppression system provider has been engaged, with implementation scheduled by the end of Q3 2025;

viii. that the insurance company provided a risk assessment in terms of article 32 and recital 79 of the Regulation:

[8] Complaint received on the 11th April 2025, and registered internally as [redacted]

Criterion	Assessment
Likelihood	Single human error, immediately identified.
Impact	Limited. No financial or special-category data involved.
Scope	The deletion affected exactly seven (7) rows. Cross-checks confirm no other data subjects were contacted.
Residual Risk	Low once automated suppression is live (scheduled Q3 2025).

ix. that the insurance company takes data privacy very seriously and fully accepts that two (2) marketing calls should never have been placed once the data subject had exercised the right to object;

x. that the incident arose from a single, easily identifiable human error during a temporary process which is now being replaced; and

xi. that decisive corrective steps already taken, together with the structural measures underway, reduce the likelihood of recurrence to a negligible level.

Further clarifications sought from the insurance company

5. By means of an email dated 19th August 2025, the Commissioner requested the insurance company to clarify the following points:

i. to confirm whether the call received by the complainant was a cold call or made using the complainant's retained personal data;

ii. to explain how the insurance company conducts marketing calls, specifically whether they are cold calls or targeted calls to individuals whose personal data the insurance company holds;

iii. to clarify whether the complainant is currently a client or was a client in the past;

iv. to provide a copy of the controller–processor agreement with the third-party company that carried out the calls on behalf of the insurance company and the full legal name of that company; and

v. to clarify whether staff and contractors receive training on compliance with data protection laws and regulations.

6. In response, the insurance company provided a copy of the signed controller-processor agreement entered into with the third-party company on the 1st January 2024. The insurance company also provided the following clarifications for the Commissioner to consider in his legal analysis:

a. *that "[t]he call received by* [the complainant] *was a cold call initiated by our outbound calling provider using randomly generated telephone numbers. No* [the insurance company] *customer or prospect records were used to place this call.* [The complainant's] *number should have been blocked by our internal suppression ("do-not-call") list. However, an outdated suppression file was provided to the calling provider for this campaign. This has been corrected"*;

b. *that "[f]or prospecting,* [the insurance company] *conducts acquisition calls only via cold calling (randomly generated numbers) performed by our provider.* [The insurance company] *does not carry out personalised marketing calls to existing or former clients using their personal data. Separately,* [the insurance company] *may contact existing clients for regulatory/servicing purposes (for instance, periodic portfolio reviews). Those servicing calls are not used for marketing";*

c. *that "[o]ur searches confirm that* [the complainant] *is not and has never been a client* [of the insurance company]. *His mobile number (with name) appears only in* [the insurance company's] *do-not-call/suppression register, which is maintained solely to honour opt-out requests and to prevent marketing calls";*

d. *that "[t]he calls were carried out on* [the insurance company's] *behalf by* [the third-party company], *acting as our processor"; and*

e. *that* "[the insurance company's] *personnel involved in marketing, sales oversight, and outsourcing management complete annual training on the GDPR and rules on electronic communications/direct marketing. Completion is mandatory and recorded. Under the Controller-Processor Agreement,* [the third-party company] *is required to ensure that all staff engaged on* [the insurance company's] *campaigns receive appropriate training and act in compliance with data protection obligations.*

LEGAL ANALYSIS AND DECISION

The roles in relation to the processing activity

7. As a first step in analysing this complaint, the Commissioner considered it necessary to identify the exact roles of the parties involved in the processing of personal data, since this determines who shall be responsible for compliance with the provisions of the Regulation. The Commissioner emphasised that understanding whether the third-party company acted as a controller or as a processor is crucial, since under the accountability principle, the controller is responsible for and must be able to demonstrate compliance with the data protection principles as set out in article 5(1) of the Regulation.

8. It therefore follows that the controller is the main entity bound by the provisions of the Regulation and has responsibility and liability in terms of compliance. Notwithstanding the fact that a processor does not process personal data on its own volition but rather on behalf of the controller, the Regulation still imposes several direct obligations upon the processor and therefore, it is essential to clearly outline the roles of the actors involved in the processing activity.

9. Accordingly, the Commissioner examined article 4(7) of the Regulation, which defines the term controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

10. The crucial aspect for assuming the role of a controller is the determination of the *'means'* and the *'purposes'* of the processing. In other words, the controller should decide, in an

autonomous manner, certain key elements about the processing and consequently, exercise decisive influence over the same processing activity. Therefore, the question *'who determines the purposes and means of the processing of personal data'* is essential to distinguish between the roles of the controller and the processor. In this regard, the European Data Protection Board (the **"EDPB"**) in the *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'* (the **"Guidelines 07/2020"**)[9] stress that *"the concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis"*[10] and *"it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing"*[11].

11. A corollary of this *'factual'* approach is that the attribution of the role of controller is based on who is effectively and concretely making decisions in relation to the purposes and means of a specific processing activity. Another essential component of the definition of *'controller'* is the object of control, which refers to the purposes and means of the processing, which is loosely translated into the *'why'* and *'how'* of the processing operation.

12. Understanding the role of the processor is equally important to correctly allocate responsibilities in terms of the provisions of the Regulation. Within this context, the Commissioner examined article 4(8) of the Regulation, which defines the role of a processor as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. Therefore, to qualify as a processor, an entity must process personal data on behalf of the controller. The decisive factor for distinguishing a processor from the controller is that a processor should not process personal data in its own interest and for the purpose of fulfilling its own objectives but should rather act on behalf of the controller on documented instructions. A processor therefore serves the interests of the controller and it is strictly bound by its instructions, having no or only very little room for making autonomous decisions and acting as an extended arm of the controller.

13. After considering these legal definitions, the Commissioner proceeded to scrutinise the submissions made by the insurance company in April and August 2025 and the copy of the

[9] European Data Protection Board, *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'*, (Version 2.1) adopted on the 7th July 2021, paragraph 12.
[10] Ibid, paragraph 21.
[11] Ibid, paragraph 52.

signed controller-processor agreement with the third-party entered into on the 1st January 2024, particularly Clause 10.1, which states that:

> *"**Both Parties, each acting as Data Controllers**, agree that in terms of personal data, each of the parties shall be responsible for data protection in accordance with their applicable laws and the General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) requirements"* [emphasis has been added].

14. Although the contract itself refers to both parties as *'Data Controllers'*, the factual and functional reality emerging from the submissions of the insurance company dated the 30th April 2025 and the 20th August 2025 shows that the third-party company was engaged to carry out outbound calls *'on behalf of'* the insurance company, using data and suppression lists provided by the insurance company. The insurance company confirmed that *"[t]he calls were carried out on* [the insurance company's] *behalf by* [the third-party company], *acting as our processor"* and that *"an outdated suppression file was provided to the calling provider for this campaign"*. These statements clearly indicate that the third-party company was acting only under the insurance company's direction and did not decide for itself the purpose or the means of the processing.

15. Subsequently, the Commissioner scrutinised the Guidelines 07/2020 wherein it is stated that *"[t]he concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract). This means **that the allocation of the roles usually should stem from an analysis of the factual elements or circumstances of the case** and as such is not negotiable"* [12] [emphasis has been added].

16. On the basis of these facts and following the functional and factual approach set out in the EDPB's Guidelines 07/2020, the Commissioner concludes that, despite the contract lists both parties as controllers, the reality of the relationship demonstrates that the insurance company determined the purposes and means of the processing (the **"controller"**), while

[12] Ibid, paragraph 12.

the third-party company merely executed those instructions. Consequently, the third-party company qualifies as a processor within the meaning of article 4(8) of the Regulation.

The Controller-Processor Agreement

17. Article 28(3) of the Regulation imposes that the relationship between the controller and the processor shall be formalised by means of *"a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller"*. This contract or legal act 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 also sets out how the relationship between a controller and processor should operate in practice[13], and binds a processor to put appropriate security measures in place for the risk to personal data[14].

18. The Commissioner considers the Guidelines 07/2020 wherein it is stated that *"[t]he degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR"*.

19. Upon reviewing the agreement submitted by the controller, the Commissioner noted that while it made general reference to compliance with data protection law, it lacked the detailed and binding obligations required under article 28(3) of the Regulation. The agreement described the parties as independent entities rather than establishing a controller-processor relationship in which one acts on behalf of the other.

20. Within this context, the Commissioner considered Guidelines 07/2020 wherein it is stated that *"[t]he degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the*

[13] Articles 28(3)(a), 28(3)(e), 28(3)(f), 28(3)(g) and 28(3)(h) of the Regulation
[14] Article 28(3)(c) of the Regulation

measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR".

Background of Complaints

21. The Commissioner proceeded to review the complainant's history of complaints against the controller. The facts gathered revealed that the complainant had previously alleged continued receipt of unsolicited communications despite having objected to the processing of his personal data under article 21 of the Regulation.

First Complaint[15]

22. The complainant's first engagement with the Commissioner occurred on the 27th February 2023, when he alleged that he had received an unsolicited call concerning insurance and retirement products offered by the controller. By means of an email dated the 26th January 2023, he had already exercised several rights under the Regulation: the right of access (article 15 of the Regulation), the right to object (article 21 of the Regulation) and the right to erasure (article 17 of the Regulation). He explained that he did not recall ever providing his personal data to the controller and requested the deletion of his personal mobile number. In its repy dated the 20th March 2023, the controller explained that the complainant had been contacted as part of a cold calling exercise carried out by its sales team, rather than on the basis of any customer relationship. An amicable settlement was reached, wherein the controller confirmed by means of an email dated the 21st March 2023, that: *"[a]s regards the delisting of his telephone number from* [the controller's] *cold calling list, I have already requested the Head of Sales to remove the number from the sequence"* **[marked and annexed as IDPC Doc 1]**.

Second Complaint[16]

[15] Ibid 5.
[16] Ibid 6.

23. The matter resurfaced on the 11th June 2024, when the complainant lodged a second complaint after receiving another unsolicited call from a third-party company acting as a Key Business Introducer on behalf of the controller. The complainant noted that his number should have already been removed following the first case and alleged that the controller had unlawfully retained and shared his personal data with a third-party without his consent. During the course of the investigation, the controller noted that the controller *"does not retain any data beyond the complainant's number on the 'Do Not Call' list, as per the agreement with them back in 2023"* **[marked and annexed as IDPC Doc 2]**.

24. In this regard, through a legally binding decision[17] dated the 10th April 2024, the Commissioner decided that:

> *"On the basis of the foregoing considerations, the Commissioner is hereby deciding that the controller has infringed article 21(2) of the Regulation for failing to instruct its sub-contracted individuals acting on its behalf to use the centralised telephone system when making calls for the purpose of direct marketing, and therefore, failed to take the appropriate action to respect the right of the complainant".*

[redacted]

Third Complaint[18]

25. Following the Commissioner's legally binding decision[19] and notwithstanding the fact that the controller informed the complainant that his number had been included in the *'Do-Not-Call'* list, the complainant was again contacted by the controller's representatives on the 4th April 2025 through two (2) separate unsolicited calls promoting insurance products. He therefore lodged a third complaint, asserting that the controller had failed to comply with the Commissioner's decision and continued to process his number for marketing purposes.

General Considerations

26. The Commissioner emphasises that the protection of natural persons in relation to the processing of personal data is a fundamental right recognised by article 8 of the Charter of

[17] Ibid 3.
[18] Ibid 8.
[19] Ibid 3.

Fundamental Rights of the European Union. The content and structure of article 8 of the Charter helps to define the constitutive elements of this fundamental right. The first paragraph broadly states that *"[e]veryone has the right to the protection of personal data concerning him or her"*. The second paragraph specifies the content of such right by elucidating that *"[s]uch data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law"*.

27. The Commissioner proceeded to examine the definition of *'personal data'* as held in article 4(1) of the Regulation, which provides that *"**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* [emphasis has been added].

Article 21(2) of the Regulation

28. In the present case, it resulted that the complainant had previously exercised his right to object to the processing of his personal data for the purpose of direct marketing in January 2023. Following that request and further to the Commissioner's legally binding decision dated the 4th October 2024[20], the controller was required to ensure that the complainant's numbers were no longer contacted for such purposes. The controller confirmed that it had acted upon this request by inserting the complainant's numbers into a centralised *'Do-Not-Call'* list, which was intended to function as a suppression mechanism across its direct marketing operations. Notwithstanding these assurances, the complainant reported that on the 4th April 2025 he was contacted twice for direct marketing purposes by individuals acting on behalf of the controller. Accordingly, the Commissioner sought to establish whether the measures taken by the controller to handle the request to objection in terms of article 21(2) of the Regulation were appropriate to give the broadest effect to the right exercised by the complainant.

29. Article 21 of the Regulation grants the data subjects the right to object to the processing of their personal data at any time in two (2) forms. Article 21(1) of the Regulation provides a

[20] Ibid 3.

general right to object whilst article 21(2) of the Regulation grants the right to object in the case of the processing for the purposes of direct marketing. In the latter case, the data subject shall have the right to request the controller to stop processing his or her personal data for direct marketing purposes without the need to demonstrate that the controller has a compelling legitimate ground to process that data. Upon receipt of a request, the controller shall ensure that the personal data of the data subject is no longer processed for the purposes of direct marketing.

30. During the course of the investigation, the controller submitted that the complainant's numbers had indeed been placed on its suppression list. However, due to a technical and procedural failure, the complainant's entries were inadvertently deleted when a new Key Business Introducer was onboarded. The error occurred because the first seven (7) rows of the suppression spreadsheet (which included the complainant's numbers) were omitted during data migration, thereby allowing the numbers to bypass the blocking mechanism and to be contacted again.

31. The Commissioner recognises that a suppression or exclusion list is an established compliance tool to ensure that a data subject who has exercised the right to object is not contacted again in the future. Such mechanisms must be implemented in a manner that gives the broadest possible effect to the objection, including through reliable technical and organisational safeguards that prevent from contacting the concerned data subjects under any circumstance. The Commissioner scrutinised the submissions of the controller and noted that the inadvertent deletion of rows during data migration meant that the complainant's objection was not respected in practice. As a consequence, the complainant was contacted again for the same purpose to which he had explicitly and unequivocally objected.

Article 5(2) & Article 24 of the Regulation

32. In this regard, article 5(2) of the Regulation sets out the principle of accountability, pursuant to which provides that the controller shall be responsible for and be able to demonstrate compliance with the principles relating to the processing of personal data as set out in article 5(1) of the Regulation. This principle of accountability stipulates an overarching compliance with the aim and purposes of the Regulation, which is essential to safeguard the rights and freedoms of the data subjects. It therefore follows that the controller is the main entity bound

by the provisions of the Regulation and has responsibility and liability in terms of compliance.

33. In connection with article 5(2) of the Regulation, article 24(1) thereof establishes an out-and-out principle of responsibility according to which *"[t]aking 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***" [emphasis has been added].

34. The principle of accountability, read in combination with the nature and scope of the responsibility of the controller, is one of the main pillars of the Regulation. Such principle places responsibility upon the controller to take pro-active action to ensure that the personal data processing activities are aligned with the data protection law, and that the same controller is in a position to effectively demonstrate compliance. Accountability is not only a legal principle but is also a crucial aspect of the fiduciary obligation between the controller and the data subject, which arises from the data subject entrusting the controller with his or her personal data. In this aspect, the Article 29 Working Party held that *"[r]esponsibility and accountability are two sides of the same coin and both essential elements of good governance.* ***Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed***"[21] [emphasis has been added].

35. In fact, recital 74 of the Regulation provides that the responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In this respect the principle of accountability, together with other more specific rules on how to comply with the Regulation and about the distribution of responsibility, require the controller to have a clear overview of the personal data undergoing processing and about the roles of the different actors in respect of the processing of such data.

[21] Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, adopted on the 13th July 2010, page 7.

36. The accountability principle is also reflected in article 28 of the Regulation, which lays down the controller's obligations when engaging a processor. In instances wherein a controller engages a processor, the overarching accountability obligation of the controller to ensure compliance with data protection principles necessitates that the controller ensures that any contract with a processor effectively enables compliance with its obligations. Article 28 of the Regulation seeks to ensure that controllers have oversight of processors engaged by them, in fact article 28(1) of the Regulation imposes an obligation on controllers to *"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"*.

37. Against this background, the Commissioner concludes that the controller's failure to enforce the exclusive use of its centralised suppression system by all the representatives, its inadequate supervision of the Key Business Introducer and its failure to address technical shortcomings in subsequent data migration exercises rendered its measures ineffective. As a result, the controller failed to give the right of the complainant its full and broadest effect and to respect his wishes not to be contacted again for the purpose of direct marketing.

[redacted]

Summary of Findings

	Article of the Regulation	Findings
1	Article 21(2) of the Regulation	The controller failed to respect the complainant's right to object to the use of his personal number for direct marketing purposes, resulting in further unsolicited communications.
2	Article 24(1) of the Regulation	The controller failed to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing of the complainant's personal data was carried out in compliance with the Regulation, particularly in the context of data

		migration and the engagement of Key Business Introducer.
3	Article 5(2) of the Regulation	The controller failed to comply with the accountability principle as it could not demonstrate effective control over the processing activities carried out on its behalf, undermining the fundamental accountability obligation placed upon it.
4	Article 28(3) of the Regulation	The controller failed to ensure that its contractual relationship with its processor complied with the requirements of article 28(3) of the Regulation.

Exercise of Corrective Powers

38. The Commissioner takes into account the toolset of corrective powers at his disposal where it results that the processing operation infringes the provisions of the Regulation. These include, *inter alia*, the power to impose an effective, proportionate and dissuasive administrative fine pursuant to the list of circumstances that refer to the features of the infringement.

39. The Commissioner notes that article 58(2) of the Regulation outlines the corrective powers that supervisory authorities may exercise in cases of non-compliance by a controller or processor. In determining whether to exercise these powers, recital 129 of the Regulation provides the following guidance: *"...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".*

40. Having carefully considered the infringements identified in this decision, the Commissioner has decided to exercise certain corrective powers under article 58(2) of the Regulation. In this regard, the Commissioner has determined that the appropriate corrective powers to address these infringements are:

a. article 58(2)(b) of the Regulation to issue a reprimand to the controller for its infringements of the Regulation identified in this decision;

b. article 58(2)(d) of the Regulation to order the controller to bring its processing into compliance with the Regulation; and

c. article 58(2)(i) of the Regulation to impose administrative fines, pursuant to article 83 of the Regulation, in response to the controller's infringements identified in this decision.

Imposition of a reprimand

41. Article 58(2)(b) of the Regulation provides that a supervisory authority shall have the power *"to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"*.

42. The Commissioner has decided to issue a reprimand to the controller for the infringements identified in this decision, aiming to deter non-compliance with the Regulation.

43. The infringements relate to the controller's failure to respect the complainant's right to object under article 21(2) of the Regulation, its failure to implement appropriate technical and organisational measures in terms of article 24(1) of the Regulation. Moreover, the controller should not ignore the fact that the accountability principle pursuant to article 5(2) of the Regulation, requires it to take proactive and demonstrable steps to ensure that all processing operations comply with the Regulation. The failure to properly oversee its representatives and to ensure that suppression mechanisms were reliably implemented, illustrates a lack of effective governance and responsibility. Additionally, the controller failed to ensure that the controller–processor agreement met the requirements enlisted in article 28(3) of the Regulation. Given the seriousness of these breaches, reprimands are appropriate in respect of such non-compliance, to formally recognise the serious nature of the infringements and to dissuade such non-compliance.

44. The reprimand is necessary and alongside the other corrective measures imposed in this decision. The Commissioner considers it appropriate to issue this reprimand to the controller to deter future similar non-compliance actions. A reprimand is proportionate in the circumstances where it does not exceed what is required to enforce compliance with the

Regulation, taking into account the serious nature of the infringements and the potential for harm to data subjects.

Order to bring processing into compliance

45. Article 58(2)(d) of the Regulation provides that a supervisory authority shall have the power *"to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period"*.

46. The Commissioner considers that, under article 58(2)(d) of the Regulation, an order should be imposed requiring the controller to bring processing into compliance by taking the following actions:

[redacted]

a. to implement robust technical and organisational safeguards to ensure that suppression lists cannot be bypassed under any circumstance, including during data migration or the onboarding of third-party business introducers;

b. to comply with the complainant's request pursuant to article 21(2) of the Regulation and therefore stop processing the complainant's personal data for such purposes in accordance with article 21(3) of the Regulation; and

c. to review and update the controller-processor agreement to ensure that it fully complies with the requirements of article 28(3) of the Regulation, clearly establishing the binding nature of the processor's obligations and detailing the scope, duration, nature and purpose of processing.

47. In light of the non-compliance identified in this decision, the Commissioner considers the order to be both necessary and proportionate, representing the minimum action required to ensure that the controller achieves full compliance in the future. While the order imposes specific remedial obligations on the controller, the reprimand serves to formally acknowledge the seriousness of the infringements, and together, these measures are deemed essential and proportionate in addressing the non-compliance outlined in this decision.

48. Accordingly, the controller is required to comply with this order **within twenty (20) days from the date of service of this decision**, and within the same period, confirm the actions taken to align its processing activities with the Regulation.

Administrative fines

49. Article 58(2)(i) of the Regulation provides that a supervisory authority shall have the power *"to impose an administrative fine pursuant to Article 83, **in addition to,** or instead of measures referred to in this paragraph, depending on the circumstances of each individual case"* [emphasis has been added]. This establishes that the Commissioner has the power to impose administrative fines either in addition to, or as an alternative to the other corrective powers specified in article 58(2) of the Regulation.

50. Article 83(1) of the Regulation provides that *"[e]ach supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*. The Commissioner therefore proceeded to examine article 83(2) of the Regulation, which provides certain criteria in deciding whether to impose an administrative fine and on the amount of the administrative fine in each individual case.

51. In applying the factors under article 83(2)(a) to (k) of the Regulation to the infringements, the Commissioner has analysed them collectively where appropriate. However, the Commissioner has considered every infringement separately when deciding whether to impose an administrative fine in respect of each infringement. Each decision is made separately, without prejudice to any factors arising from other infringements. For clarity, the decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine, where applicable, is independent and specific to the circumstances of each infringement.

Article 83(2)(a) of the Regulation

52. Due regard was given to article 83(2)(a) of the Regulation, which refers to *"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".

Nature of Processing

53. Insofar as the nature of the infringement is concerned, the Commissioner observed that the controller failed to give the right of the complainant its full broadest effect. The rights of the data subjects as set forth in Chapter III of the Regulation are the fulcrum and the basis of the law and their role is crucial to give the data subjects control over their personal data. It is indeed the intention of the legislator to sanction any infringement of the data subjects' rights in an appropriate and effective manner, considering that these rights constitute the fundamental basis on the strength of which protection and control are afforded to data subjects with regard to the processing of their personal data.

Purpose of the Processing

54. The Commissioner established that the processing was carried out for direct marketing purposes, specifically to promote insurance and retirement products. However, the Commissioner noted that the commercial interests of a controller can never override the fundamental rights of data subjects. The Commissioner further noted that the Regulation grants data subjects an absolute right to object to the processing of their personal data for direct marketing purposes, as stipulated in article 21(2) of the Regulation. Once this right is exercised, any further contact for marketing purposes becomes unlawful.

Affected Data Subjects

55. In relation to the number of affected data subjects, the Commissioner determined that this case concerns a single complainant.

Level of Damage

56. Another factor that needs to be taken into account for the purpose of determining the gravity of the infringement is the level of damage suffered or likely to be suffered and the extent to which the infringement may affect the rights and freedoms of the data subjects. According

to the EDPB's *'Guidelines on the application and setting of administrative fines'*[22] (the **"Guidelines 04/2022"**), *"the reference to the "level" of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved"*[23].

57. It is indeed the intention of the legislator to sanction any infringement of the data subjects' rights in a severe manner, considering that such rights are fundamental instruments at the disposal of the data subjects, which enable them to exercise control over their personal data within a stipulated time-frame. Thus, whilst assessing the gravity of the infringement, the Commissioner has also taken into account that the negligent behaviour of the controller hindered the complainant from exercising his right.

Duration of the Infringement

58. Another factor which was considered by the Commissioner is the duration of the infringement. In accordance with the Guidelines 04/2022, the duration of the infringement may generally attribute more weight if the infringement is of a longer duration.

59. In the present case, the infringement spans from the initial objection lodged in January 2023 to the most recent unsolicited calls received in April 2025, a period of more than two (2) years. This extended duration highlights the controller's failure to take timely and effective corrective measures, despite repeated opportunities and a legally binding decision.

Nature and Gravity of the Infringement

60. Considering the specific circumstances of the case, read in light of article 83(2)(a) of the Regulation, the Commissioner placed substantial emphasis on the following key factors: (i) the nature of the processing; (ii) the purpose of the processing; (iii) the level of damage; and (iv) the duration of the infringement. Collectively, these factors serve as indicators of the gravity of the infringement.

[22] European Data Protection Board, *'Guidelines 04/2022 on the calculation of administrative fines under the GDPR'*, (Version 2.1) adopted on the 24th May 2023, paragraph 19.
[23] Ibid, paragraph 55.

Article 83(2)(b) of the Regulation

61. Article 83(2)(b) of the Regulation provides that one of the general conditions is the *"intentional or negligent character of the infringement"*. The Commissioner examined whether the character of the infringement committed by the controller was intentional or negligent.

62. In its Guidelines, the Article 29 Working Party (the predecessor of the EDPB) specifically refers to and distinguishes between infringements of an intentional character and infringements of a negligent character, stating 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"*[24]. In particular, the Article 29 Working Party Guidelines cite '*human error*' as a specific example of a circumstance that may be indicative of negligence.

63. After identifying the facts gathered during the course of the investigation and considering the controller's repeated failure to comply with the complainant's requests to object from the processing of personal data for marketing purposes, the Commissioner determined that the controller had acted negligently. This negligence arose from a lack of adequate oversight in ensuring that any third-party company engaged to process data on its behalf provided sufficient guarantees to implement appropriate technical and organisational measures.

64. The Commissioner further notes that, although an agreement existed between the controller and the third-party company, it did not comply with the requirements of article 28(3) of the Regulation. By failing to ensure that the agreement specified the subject matter, duration, nature and purpose of the processing, as well as the processor's binding obligations, the controller did not exercise the necessary oversight and due diligence required by the accountability principle under article 5(2) of the Regulation. It must be emphasised that accountability ultimately rests with the controller, and consequently, any negligence or failure to comply with the provisions of the Regulation by the processor(s) remains the controller's responsibility.

[24] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, adopted on the 3rd October 2017, page 11.

Article 83(2)(c) of the Regulation

65. The Commissioner examined article 83(2)(c) of the Regulation, which addresses *"any action taken by the controller or processor to mitigate the damage suffered by data subjects"*. According to the Guidelines 04/2022:

> *"The measures adopted must be assessed, in particular, with regard to the element of timeliness, i.e. the time when they are implemented by the controller or processor, and their effectiveness. In that sense, measures spontaneously implemented prior to the commencement of the supervisory authority's investigation becoming known to the controller or processor are more likely to be considered a mitigating factor, than measures that have been implemented after that moment"*[25].

66. The Commissioner noted that, following the complainant's first objection in January 2023, the controller placed the complainant's mobile numbers on a *'Do-Not-Call'* list. This was intended to prevent further marketing calls, however the controller failed to ensure that this mechanism remained effective over time. In this regard, the Commissioner analysed the controller's submissions dated 30th April 2025, wherein it was explained that when a new data migration exercise was carried out, several entries, including that belonging to the complainant, were mistakenly deleted from the suppression list, which meant that the system no longer recognised his number as one that should not be contacted.

67. The Commissioner acknowledges that creating the *'Do-Not-Call'* list was initially a reasonable step to prevent further contact with the complainant. However, this measure ultimately enabled the same issue to recur, thereby undermining its intended positive effect.

68. Accordingly, the Commissioner finds that the controller's actions cannot be regarded as an effective mitigating factor within the meaning of article 83(2)(c) of the Regulation. Although the controller initially took steps to prevent recurrence, these were not implemented or maintained in a reliable manner and therefore failed to mitigate the impact on the complainant.

Article 83(2)(d) of the Regulation

[25] Ibid 22, paragraph 76.

69. Pursuant to article 83(2)(d) of the Regulation, the Commissioner must give due regard to the degree of responsibility of the controller, taking into account the technical and organisational measures implemented by the controller pursuant to articles 25 and 32 of the Regulation. Pursuant to the Guidelines 04/2022, the Commissioner must consider the following pertinent matters:

> *"Following Article 83(2)(d), the degree of responsibility of the controller or processor will have to be assessed, taking into account measures implemented by them pursuant to Articles 25 and 32 GDPR. In line with Guidelines WP253, "**the question that the supervisory authority must then answer is to what extent the controller 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation**"*[26] **[emphasis has been added].**

70. In this case, the controller had introduced certain organisational mechanisms, however the Commissioner's investigation established that these measures were ineffective. The Commissioner considers that these deficiencies constitute a clear infringement of article 24(1) of the Regulation, as the controller failed to implement and maintain appropriate technical and organisational measures to ensure that processing was carried out in accordance with the Regulation. In addition, the controller failed to establish a compliant controller-processor agreement as required under article 28(3) of the Regulation. Consequently, the controller failed to properly supervise the processor's activities. These deficiencies also amount to a breach of the accountability principle under article 5(2) of the Regulation, which requires the controller not only to comply with the principles laid down in article 5(1) of the Regulation, but also to be able to demonstrate such compliance. In this case, the controller could not demonstrate that it had taken sufficient or effective steps to ensure that objections to direct marketing were respected in practice.

71. In this regard, the Commissioner considers that the controller did not act with the level of diligence and responsibility expected under the Regulation. The recurring nature of the infringement, together with the fact that the same issue had already been the subject of a

[26] Ibid 22, paragraph 77.

previous investigation and a legally binding decision[27], indicates that the controller did not ***'[do] what it could be expected to do'***[28] to ensure compliance. While the Commissioner acknowledges that a remedial action was taken, these steps followed the lodging of the third complaint and therefore cannot offset the gravity of the breach. The repeated non-compliance with a prior legally binding decision[29] constitutes an aggravating factor under article 83(2)(e) of the Regulation. For these reasons, the Commissioner concludes that the controller failed to uphold its duties under article 5(2) and article 24(1) of the Regulation and article 28 thereof.

Article 83(2)(e) of the Regulation

72. Article 83(2)(e) of the Regulation provides for *"any relevant previous infringements by the controller or processor"*. The Guidelines 04/2022 outlines that *"[e]ven though all prior infringements might provide an indication about the controller's or processor's general attitude towards the observance of the GDPR, infringements of the same subject matter* ***must be given more significance, as they are closer to the infringement currently under investigation, especially when the controller or processor previously committed the same infringement (repeated infringements). Thus, same subject-matter infringements must be considered as more relevant than previous infringements concerning a different topic"***[30] [emphasis has been added].

73. In this case, the Commissioner notes a clear and repeated failure to respect the complainant's right to object to direct marketing under article 21(2) of the Regulation.

74. The Commissioner noted that the complainant first lodged a complaint in February 2023[31], after receiving marketing calls despite never having given consent. This case was resolved amicably after the controller confirmed that the complainant's number would be removed from its cold-calling list. Subsequently, in June 2024, the complainant filed a second complaint[32] after receiving another unsolicited call. This led the Commissioner to issue a

[27] Ibid 3.
[28] Ibid 22, paragraph 77.
[29] Ibid 3.
[30] Ibid 22, paragraph 88.
[31] Ibid 5.
[32] Ibid 6.

legally binding decision dated the 10th April 2024[33], wherein it was held that the controller had infringed article 21(2) of the Regulation, and despite this, the complainant was contacted once again in April 2025, leading to the current complaint[34].

75. The Commissioner therefore finds that the three (3) complaints all relate to the same right, the same controller and the same kind of processing activity. This consistent pattern of non-compliance clearly indicates that the controller failed to take adequate corrective action or to implement sufficient organisational and technical measures to prevent a similar infringement from happening. Accordingly, this falls within the scope of article 83(2)(e) of the Regulation, as it demonstrates a continued disregard for the controller's obligations and is therefore regarded as an aggravating factor in the assessment and determination of the appropriate sanction.

76. The Commissioner further notes that such repeated infringements undermine the effectiveness of data subject rights and therefore, the complainant should not have been required to file successive complaints for his right to be respected.

[redacted]

Article 83(2)(f) of the Regulation

77. Another factor that needs to be taken into account when determining the quantum of the fine is the degree of cooperation with the Commissioner in order to remedy the infringement and mitigate the possible adverse effects of the infringement. In such case, the Commissioner noted that the controller demonstrated cooperation by promptly complying with the order to provide the information requested by the Commissioner. However, this cooperation does not serve as a mitigating factor, as it is the controller's obligation in terms of article 31 of the Regulation to cooperate with the Commissioner in the performance of his investigative tasks.

Article 83(2)(g) of the Regulation

[33] Ibid 3.
[34] Ibid 8.

78. The personal data affected in this case consisted of the complainant's mobile number, which is information that directly identifies[35] a specific person and therefore clearly falls within the definition of personal data in article 4(1)[36] of the Regulation.

Article 83(2)(h) of the Regulation

79. Another factor that must be considered by the supervisory authority is the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller notified the infringement. After assessing article 83(2)(h) of the Regulation, the Commissioner noted that the infringement became known to him as a result of a complaint lodged by the affected data subject pursuant to article 77(1) of the Regulation.

Article 83(2)(i) of the Regulation

80. The Commissioner noted article 83(2)(i) of the Regulation stating that *"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"*. In this case, no corrective measures have previously been ordered against the controller concerning the subject matter of the decision. As a result, this factor is neither aggravating nor mitigating in these circumstances.

Article 83(2)(j) of the Regulation

81. The Commissioner also considered article 83(2)(j) of the Regulation, which provides for adherence to approved codes of conduct under article 40 or approved certification mechanisms under article 42 of the Regulation. These considerations do not apply in this case.

---

[35] Pursuant to recital 26 of the Regulation *"[...] to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments [...]"*.

[36] Article 4(1) of the Regulation defines personal data as *"any information relating to an identified or identifiable natural person"*.

Imposition of an administrative fine

82. In deciding whether to impose an administrative fine in respect of each infringement, the Commissioner had regard to the factors outlined in article 83(2)(a) to (j) of the Regulation cumulatively. However, each infringement has been assessed separately when applying those factors, deciding whether to impose a fine and determining its amount. The Commissioner has also had regard to the effect of a reprimand and order to bring processing into compliance, ensuring that they contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements.

83. The Commissioner considers that a reprimand is of significant value in dissuading future non-compliance, as a formal recognition of the controller's identified infringements. The order to bring processing into compliance should result in the controller's immediate action to remedy the identified infringements. However, the Commissioner considers that these measures alone are not sufficient in the circumstances to ensure compliance, and therefore, he finds that imposing two (2) administrative fine is appropriate, necessary and proportionate to ensure compliance with the provisions of the Regulation.

84. The infringed articles include a fundamental principle of the Regulation under article 5(2) of the Regulation, which is the controller's requirement to not only be responsible but also to be able to demonstrate compliance with the data protection principles enlisted in article 5(1) thereof; and the obligation under article 21(2) of the Regulation to respect a data subject's right to object to the processing of personal data for direct marketing purposes. Additionally, the controller failed to comply with article 24(1) of the Regulation, which places an obligation on the controller to implement appropriate technical and organisational measures to always ensure that processing is carried out in accordance with the Regulation; and the obligation under article 28(3) of the Regulation to ensure that processing by a processor is governed by a binding written agreement containing the elements required by the provisions of the Regulation. The Commissioner considers that administrative fines are appropriate, necessary and proportionate to dissuade future non-compliance by the controller.

85. In reaching the conclusion that the imposition of an administrative fine is necessary, the Commissioner gave particular regard to the nature, gravity and duration of the

infringements, including the repeated failures of the controller to respect the complainant's right to object to direct marketing under article 21(2) of the Regulation, as well as the continuing lack of effective organisational and technical measures under article 24(1) of the Regulation and the accountability principle in article 5(2) of the Regulation. The Commissioner also took into account the degree of negligence on the part of the controller in failing to ensure that its centralised suppression list was consistently used and maintained, including during data migration exercises, as well as the failure to supervise representatives and third-party companies, in line with articles 83(2)(b) and (d) of the Regulation. Further consideration was given to the absence of effective measures to mitigate the impact of these repeated infringements on the complainant, in accordance with article 83(2)(c) of the Regulation. The Commissioner has balanced these factors with the mitigating factors identified above, while also considering the toolbox of corrective powers available under article 58(2) of the Regulation.

Article 83(3) of the Regulation

86. Having completed the Commissioner's assessment of whether or not to impose a fine and its amount, it is necessary to consider article 83(3) of the Regulation to determine if there are any factors that might require the adjustment of the fines. The Commissioner noted article 83(3) of the Regulation providing that *"[i]f a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for* ***the gravest infringement****"* [emphasis has been added].

87. In this case, the identified infringements arise from linked processing operations, requiring the Commissioner to assess whether the total fine should be capped based on the gravest infringement. The infringements of article 5(2) of the Regulation as well as article 24(1) thereof, and article 21(2) of the Regulation fall under article 83(5) of the Regulation, which allow for fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher. Since all the infringements identified in this case fall under the same higher category of gravity, the overall fine imposed shall not exceed the maximum limit applicable to infringements under article 83(5) of the Regulation.

Categorisation of the infringements

88. As noted in the EDPB's Guidelines 04/2022[37], article 83(4) to article (6) of the Regulation establish different levels of infringement severity. The Guidelines 04/2022 state that *"[w]ith this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be"*. The categorisation of infringement under article 83(4) or (5) of the Regulation, is a relevant consideration in assessing the seriousness of the infringement in this case. The infringement of article 5(2) of the Regulation found in this case, relates to the basic principles of the processing and is ascribed considerably greater significance, with the legislator providing for, in general, maximum administrative fines.

Seriousness of the infringement pursuant to articles 83(2)(a), (b) and (g) of the Regulation

89. The EDBP's Guidelines 04/2022 state that the factors assessed under article 83(2)(a), article 83(2)(b) and article 83(2)(g) of the Regulation determine the seriousness of an infringement[38]. It outlines that *"[t]he assessment of the factors above determines the seriousness of the infringement as a whole. This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole"*[39].

90. Under article 83(2)(a) of the Regulation, the infringements are of a serious nature, as they concern the repeated failure to respect a data subject's right and the controller's continued non-compliance with its obligations under articles 24(1) and 5(2) of the Regulation. The infringements were of prolonged duration, extending over a period of more than two (2) years and involving three (3) separate complaints relating to the same issue and the same data subject. In assessing the nature of the personal data affected under article 83(2)(g) of the Regulation, the Commissioner notes that the processing does not impose a high risk to the rights and freedoms of the individual, however it constitutes personal data within the meaning of article 4(1) of the Regulation. Additionally, the controller was also negligent to

[37] Ibid 22, paragraph 50
[38] Ibid 22, paragraph 59.
[39] Ibid 22, paragraph 64.

a medium degree with respect to the infringements, as assessed under article 83(2)(b) of the Regulation. Therefore, balancing these factors, the Commissioner considers that the infringements are of a medium level of seriousness.

Imposing an effective, dissuasive and proportionate fine

91. Article 83(1) of the Regulation requires fines to be effective, proportionate and dissuasive in each individual case. As the Guidelines 04/2022 also say that this *"does not dismiss a supervisory authority from the responsibility to carry out a review of effectiveness, dissuasiveness and proportionality at the end of the calculation"*[40]. Therefore, article 83(1) of the Regulation will be reconsidered at the conclusion of this calculation.

Aggravating and mitigating circumstances

92. Article 83(2)(a), article 83(2)(b) and article 83(2)(g) of the Regulation were considered above in relation to the starting point for the calculation of the fine. In line with the approach suggested in the Guidelines 04/2022[41], this section considers the aggravating or mitigating impact of the remaining criteria in article 83(2) of the Regulation. Regarding article 83(2)(c) of the Regulation, the controller initially took steps to include the complainant's numbers on a *'Do-Not-Call' list* following his objection in January 2023. However, the effectiveness of this measure was not maintained, as the complainant's details were later deleted during a data migration exercise, resulting in further unsolicited calls. The Commissioner therefore considers that, although the controller adopted measures intended to mitigate harm, these were undermined by systemic deficiencies in data governance and a lack of effective oversight, rendering them neither ineffective within the meaning of article 83(2)(c) of the Regulation.

93. Concerning article 83(2)(d) of the Regulation, it was noted that the controller had a high degree of responsibility for the infringements. This is considered an aggravating factor of moderate weight, considering that the controller did not do *'what it could be expected to do'* in the circumstances assessed above and thus failed to ensure effective use of the measures

[40] Ibid 22, paragraph 64.
[41] Ibid 22, paragraph 70

implemented. Considering that the controller did take some steps to seek to ensure compliance, the weighting attributed to this factor is moderate rather than high.

94. In relation to article 83(2)(e) of the Regulation, the Commissioner notes a clear pattern of repeated infringements and despite a previous legally binding decision[42] on the same matter, the controller once again failed to respect the complainant's data protection right. This reflects a continuing disregard for regulatory obligations and is therefore considered an aggravating factor.

95. Under article 83(2)(f) of the Regulation, the Commissioner acknowledges that the controller cooperated with the Commissioner throughout the investigation and provided the information requested in a timely manner. Having said that, the controller has a general obligation to cooperate under article 31 of the Regulation and therefore, this factor is considered to be neither mitigating nor aggravating.

96. The infringement came to the Commissioner's attention via a data subject's complaint, as per article 83(2)(h) of the Regulation. Finally, the Commissioner deems articles 83(2)(i), (j) and (k) of the Regulation to be neither mitigating nor aggravating.

97. For the reasons outlined above and with particular regard to article 83(2) of the Regulation and the Guidelines 04/2022[43], the Commissioner has decided to impose the following administrative fines on the controller:

i. **five hundred euro (€500)** for the infringement of article 5(2) and article 24(1) of the Regulation; and

ii. **five hundred euro (€500)** for the infringement of article 21(2) of the Regulation.

Article 83(1) of the Regulation: Effectiveness, proportionality and dissuasiveness

a. Effectiveness

[42] Ibid 3.
[43] Ibid 3.

98. The Commissioner believes that for a fine to be *'effective'*, it must be substantial enough to influence the controller or processor, ensuring that compliance with the Regulation becomes a key factor in governance and high-level decision-making. In this case, the infringements involve core obligations of the Regulation, including the accountability principle under article 5(2) of the Regulation, the right to object under article 21 of the Regulation, and the responsibility to implement appropriate technical and organisational measures under article 24 of the Regulation. Thus, considering these factors, the Commissioner deems the imposed fines effective, requiring no further adjustment.

b. Dissuasiveness

99. For a fine to be *'dissuasive'*, it must deter both the specific controller or processor involved and others engaging in similar processing operations from repeating the misconduct. The Commissioner considers the imposed fines sufficient to achieve this deterrent effect. Each infringement is serious in nature and gravity, as outlined in article 83(2)(a) of the Regulation. Violations of fundamental principles of the Regulation, including the accountability principle demand strong corrective measures. The Commissioner emphasises that non-compliance with these principles must be firmly addressed to uphold data subjects' rights and reinforce the importance of adherence. Therefore, the imposition of administrative fines is both appropriate and necessary to prevent future non-compliance.

[redacted]

100. The controller's failure to respect the complainant's data protection right under article 21(2) of the Regulation, its inability to maintain the integrity of the suppression list during data migration and the lack of effective oversight over its third-party companies demonstrate a serious disregard for the obligations emanating from the Regulation. This negligence underscores the necessity of administrative fines to ensure that the controller takes its responsibilities seriously and implements the necessary corrective measures.

101. The Commissioner considers that the imposition of administrative fines will encourage the controller and other similar entities to take appropriate action to prevent further infringements. In this instance, the Commissioner notes that the controller had already been found to have committed prior infringements. The repetition of these infringements, despite prior findings, demonstrates a failure on the part of the controller to adequately address compliance shortcomings. Given the repeated and negligent character of the infringements

and the controller's failure to uphold its obligations, the Commissioner considers that the imposition of dissuasive administrative fines is necessary to ensure future compliance.

c. Proportionality

102. *'Proportionality'* is a fundamental principle of EU law, requiring that any measure pursues a legitimate objective, is appropriate to achieve that objective and does not exceed what is necessary. The objectives of the administrative fines in this case are to re-establish compliance with the provision of the Regulation and to sanction the controller's infringements.

103. The Commissioner considered the nature, gravity and duration of the infringements, he deems the administrative fines proportionate to ensuring compliance. The controller repeatedly failed to respect the complainant's right to object under article 21(2) of the Regulation and failed to implement and maintain effective technical and organisational measures in accordance with articles 24(1) and 5(2) of the Regulation. In light of this, the Commissioner finds the administrative fines appropriate to address the controller's infringement and promote future compliance. The administrative fines do not exceed what is necessary to enforce compliance with the identified infringements in this decision.

[redacted]

SUMMARY OF ENVISAGED ACTION

In summary and on the basis of the foregoing considerations, the Commissioner is hereby exercising on the controller the following corrective powers under article 58(2) of the Regulation:

i. a reprimand pursuant to article 58(2)(b) of the Regulation regarding the infringements identified in this decision, particularly:

a. the repeated failure to respect the complainant's right to object to the processing of his personal data for direct marketing purposes, in violation of article 21(2) of the Regulation;

b. the failure to implement and maintain appropriate technical and organisational measures to ensure that the processing was carried out in

accordance with articles 24(1) of the Regulation, thereby demonstrating non-compliance with the accountability principle set forth in article 5(2) of the Regulation; and

c. the failure to ensure that the contractual relationship with its processor complied with the requirements of article 28(3) of the Regulation, thereby lacking the necessary binding framework to govern the processor's obligations.

ii. an order pursuant to article 58(2)(d) of the Regulation, requiring the controller to bring processing into compliance by taking the following actions:

a. to implement robust technical and organisational safeguards to ensure that suppression lists cannot be bypassed under any circumstance, including during data migration exercises or the onboarding of third-party companies;

b. to comply with the complainant's request under article 21(2) of the Regulation and therefore no longer process the complainant's personal data for direct marketing purposes in accordance with article 21(3) of the Regulation; and

c. to ensure that the contractual agreement with any third-party processors or any Key Business Introducer is fully compliant with article 28(3) of the Regulation.

The aforementioned orders shall be complied without undue delay and by no later than twenty (20) days from the date of service of this legally binding decision and confirmation of the action taken shall be notified to the Commissioner immediately thereafter.

iii. the imposition of two (2) effective, proportionate and dissuasive administrative fines pursuant to article 58(2)(i) of the Regulation, as follows:

a. five hundred euro (€500) for infringing article 5(2) and article 24(1) of the Regulation; and

iii. five hundred euro (€500) for infringing article 21(2) of the Regulation.

The total amount of the fine shall be paid within twenty (20) days from the date of service of this legally binding decision.

Dr Reno Borg
Information and Data Protection Commissioner

Today, the 4th of May 2026.

Right of Appeal

In terms of article 26(1) of the Data Protection Act (Cap 586 of the Laws of Malta), *"any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Tribunal within twenty days from the service of the said decision as provided in article 23".*

An appeal to the Information and Data Protection Appeals Tribunal shall be made in writing and addressed to:

The Secretary
Information and Data Protection Appeal Tribunal
158, Merchants Street
Valletta.