

**DATA PROTECTION ACT 2018 (PART 6, SECTION 155)**

**SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER**

**MONETARY PENALTY NOTICE**

To: Easylife Limited

Of: 94 Orchard Gate, Greenford, England, UB6 0QP

**Introduction and Summary**

1. This Information Commissioner ("the Commissioner") has decided to issue Easylife Limited ("Easylife") with a monetary penalty under section 155 of the Data Protection Act 2018 ("the DPA"). The penalty notice imposes an administrative fine on Easylife, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 ("the GDPR"). The amount of the penalty is £1,350,000 (one million, three hundred and fifty thousand pounds).
2. The penalty is in relation to contraventions of Article 5(1)(a) of the GDPR and an ongoing incident during the period of 1 August 2019 to 19 August 2020 ("the relevant period") affecting personal data processed by Easylife during the relevant period ("the Incident")<sup>1</sup>.
3. For the reasons set out in this Monetary Penalty Notice, the Commissioner has found that Easylife failed to process personal data in

---

<sup>1</sup> The applicable legislation at the time of the Incident was the (EU) GDPR. The Commissioner was at the material time the supervisory authority in respect of the (EU) GDPR.

relation to data subjects lawfully, fairly, and in a transparent manner, as required by Article 5(1)(a) GDPR.

4. This Notice explains the Commissioner decision, including the Commissioner's reasons for issuing the penalty and for the amount of the penalty.

## **Legal Framework**

### **Obligations of the Controller**

5. Easylife is a controller for the purposes of the GDPR and the DPA, because it determines the purposes and means of processing of personal data (GDPR Article 4(7)).

6. "Personal data" is defined by Article 4(1) of the GDPR to mean:

*"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 a 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."*

7. "Processing" is defined by Article 4(2) of the GDPR to mean:

*"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by*

*automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

8. Article 4(4) of the GDPR defines profiling:

*"profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"*

9. Article 9 GDPR prohibits the processing of "*special categories of personal data*" unless certain conditions are met. The special categories of personal data subject to Article 9 include "*data concerning health or data concerning a natural person's sex life or sexual orientation*".
10. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the GDPR. Article 5(2) makes clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".
11. In particular, controllers are required to process personal data in relation

to data subjects lawfully, fairly, and in a transparent manner, as required by Article 5(1)(a) of the GDPR. Article 5(1)(a) ("lawfulness, fairness and transparency") stipulates that:

*"Personal data shall be [...] processed lawfully, fairly and in a transparent manner in relation to the data subject"*

12. Article 13 of the GDPR requires information to be provided where personal data are collected from the data subject. Article 13(1)(3) provides:

*"Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing"*

13. Article 13(3) of the GDPR requires:

*"Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."*

14. Section 1 of Chapter 4 of the GDPR (namely Articles 24-31) addresses the general obligations of controllers and processors. Article 24 sets out the responsibility of controllers for taking appropriate steps to ensure and be able to demonstrate that processing is compatible with the GDPR.

Articles 28-29 make separate provision for the processing of data by processors, under the instructions of the controller.

## **The Commissioner's Powers of Enforcement**

15. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the GDPR.
16. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.
17. By Article 58(2)(d) of the GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) he has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.
18. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective, proportionate, and dissuasive in each individual case. Article 83(2) goes on to provide that:

*"When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*

- (a) the nature, gravity and duration of the*

*infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*

*(b) the intentional or negligent character of the infringement;*

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

*(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*

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

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

*(g) the categories of personal data affected by the infringement;*

*(h) the manner in which the infringement became known to the supervisory authority, in particular*

*whether, and if so to what extent, the controller or processor notified the infringement;*

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

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

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

19. Article 83(5) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 5 GDPR on the controller and processor will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.
20. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner<sup>2</sup>. Section 155 of the DPA sets out the matters to which the Commissioner must have regard when deciding whether to

---

<sup>2</sup> Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR.

issue a penalty notice and when determining the amount of the penalty and provides that:

*"(1) If the Commissioner is satisfied that a person—*

*(a) has failed or is failing as described in section 149(2) ...,*

*the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.*

*(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—*

*(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR."*

21. The failures identified in section 149(2) DPA 2018 are, insofar as relevant here:

*"(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—*

*(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*

*...;*

*(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors) [...]"*

22. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

*"(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice."*

### **The Commissioner's Regulatory Action Policy**

23. Pursuant to section 160(1) DPA, the Commissioner published his Regulatory Action Policy ("RAP") on 7 November 2018.
24. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described in the RAP from page 27 onwards. In particular, the RAP sets out the following five-step process:
- a. Step 1. An 'initial element' removing any financial gain from the

breach.

- b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2) - (4) DPA.
- c. Step 3. Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.
- d. Step 4. Adding in an amount for deterrent effect to others.
- e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

## **Circumstances of the Failure: Facts**

### **General Background**

25. This Penalty Notice does not purport to identify exhaustively each and every circumstance and document relevant to the Commissioner's investigation. The circumstances and documents identified below are a proportionate summary.
26. Easylife is a company based which sells household products through catalogues. The brand was founded in 1992, Easylife was incorporated on 3 September 2004 (at that date "Easylife Group Limited"). Easylife has one active director registered at Companies House, Mr Gregory Grant Caplan, who is the Chief Executive Officer. Mr Caplan is also a director of "Easylife Holdings Limited", which is registered as a person

of significant control of Easylife.

## **Discovery and Reporting of the Breach**

27. The Information Commissioner's Office ("ICO") conducted [REDACTED] [REDACTED] due to the potential of direct marketing aimed at exploiting the Covid-19 pandemic, which led to an investigation into [REDACTED] [REDACTED] ("[REDACTED]"), a telemarketing company promoting funeral plans during the pandemic. This in turn led the Commissioner to investigate Easylife, because [REDACTED] conducted outbound calling for Easylife. The Commissioner's investigation into Easylife initially concerned potential contraventions of the PECR, and that initial investigation raised concerns of potential contraventions of the GDPR, which the Commissioner then investigated separately.
28. The Easylife Health telemarketing campaign was conducted by a third-party [REDACTED] ("[REDACTED]"). The "trigger products" consisted of 122 different items sold in the Easylife catalogue. Once an individual had purchased one of the trigger products from Easylife itself, this would trigger a marketing call to the individual by [REDACTED] using the data of which Easylife was the controller. Easylife linked the trigger products to several health conditions which Easylife inferred that the customer was likely to have, which Easylife would then use as an opportunity to attempt to sell the individual health supplement products which were alleged to help the inferred health issues. Easylife explained that the selection of an individual to receive a marketing call was based solely on transactional data and that the data was provided to the call centre operated by [REDACTED] on a weekly basis, with the selection of which individuals would receive calls made on the basis of what products they had previously purchased. Easylife stated that individuals who had previously opted out of

marketing calls were removed from the call lists.

29. Easylife provided the ICO with marketing scripts selling glucosamine, Cannabidiol, prostaphytol patches and bio-magnetic joint patches. Easylife explained that the majority of the calls made during the relevant period had been targeted at individuals who had been inferred to have arthritis, for instance, a purchase of one of 80 of the 122 trigger products would lead Easylife to infer that the customer had arthritis who may then call to sell them glucosamine patches. Glucosamine is a supplement which is allegedly therapeutic for individuals with arthritis. The wording of the calling scripts was clearly targeted to individuals with the health conditions which Easylife was inferring. For example, the sales calls marketing glucosamine to data subjects inferred to have arthritis said:

*"Good morning, may I speak to XYZ please – Good morning my name is XYZ and I am one of the Health Advisors giving you a quick call from Easy Life. It is just a quick call as you ordered recently one of our \_\_\_\_\_. Can I ask, did you order it to help with arthritis in the \_\_\_\_\_, or is it an injury to the \_\_\_\_\_?"*

30. The script then posed questions about the arthritis, such as how long the individual had had it, its location, the manifestation of symptoms, and its effects on the individual. Then a sales pitch commenced:

*"So do you mind if I make a simply suggestion? Many people who suffer with Arthritis will wear Glucosamine Joint Patches. Glucosamine is a natural ingredient that our own bodies produce up to the age of 30, then as we get older our bones are less protected and through wear and tear over the years, the bones*

*and joints start to grind together which is the main cause of pain, swelling and stiffness.”*

31. The Commissioner became concerned that using data about purchasing transactions in order to make inferences about health conditions could constitute profiling, and the inferences made about health conditions could indicate processing of special category data. A sale of glucosamine patches to an individual who had previously ordered a trigger product from which Easylife had inferred that the individual probably had arthritis was therefore ostensibly linked to the success of the profiling which Easylife had undertaken.
32. The transactional purchase data of Easylife’s customers was personal data. When Easylife used that transactional data to influence its decisions on which customers to subject to telemarketing, this constituted profiling. When Easylife used the transactional data to influence its decisions on which products to market to which customers, based on its inferences about a health condition which they were likely to have, that constituted the processing of special category data, irrespective of the level of statistical confidence which Easylife had in the profiling which it had done.
33. Easylife relied on its own legitimate interests as the basis for conducting this processing, using a small section of the Easylife privacy policy which stated how personal data would be used:

*“How will we use the information we collect about you?”*

*We will do the following with your personal information.*

- *Store and use it to fulfil any order or service you’ve*

*ordered from.*

- *Maintain is as evidence of your history with us.*
- *\*Keep you informed about the status of your orders and provide updates or information about associated products or additional products, services, or promotions that might be of interest to you.*
- *\*Notify you of any product recalls or provide other information concerning products you have purchased.*
- *\*Improve and develop the products or services we offer by analysing your information.*
- *\*As customers or subscribers, we will sent you our catalogues and information by post or email and may telephone offering services or products."*

34. Individuals were not informed by Easylife that their information would be used for profiling them. Article 13 of GDPR requires data controllers to inform individuals of the type of processing which will occur. Easylife did not put in place the steps necessary to allow them to process transactional sales data for the purposes of inferring health data and then making targeted marketing calls for the purpose of selling items which Easylife had decided were relevant to the inferred health condition.

35. Easylife stated that no inferred health data was stored against any individual because only transactional data was and that legitimate interest assessments ("LIAs") had been carried out for the telephone marketing campaigns. Easylife stated that the marketing campaign included some calls intended to sell face masks during the pandemic.

36. Easylife provided the Commissioner with a LIA, which it said had also

been provided to the Commissioner in 2019 in a previous unrelated investigation. The LIA focused generally on Easylife cards and clubs and was not specific to the Easylife Health campaign. The LIA document contained 15 "queries", either a positive or negative response, some guidance and a note on each query. Queries included, "Would processing involve special categories of personal data?" which Easylife had answered negatively, stating, "No these are generic offers available for all customers." In response to the query, "Would customers expect their data to be used for this purpose?", Easylife had answered affirmatively on the basis that they had informed individuals of the purpose in their privacy policy. Easylife should have been aware from the LIA that the Health campaign would not be compliant with the GDPR, because it had asked itself questions which, if answered accurately, would have revealed the contravention. Easylife relied on an LIA which related to a different marketing campaign, which did not involve profiling customers, as the basis for the Health campaign, which did involve profiling customers.

37. The data processing agreement between Easylife and [REDACTED] covered confidentiality, security, sub-contracting and termination but omitted any reference to the type of data processing which would occur.

### **Reporting the Breach to the Information Commissioner**

38. One hundred and forty-five thousand, four hundred (145,400) individuals were profiled for inferred health conditions. Zero complaints were made to the ICO, although this was unsurprising to the Commissioner because the contraventions involved invisible processing about which Easylife never informed the individuals, with the consequence that the individuals could not know that processing of their

personal data and their special category data was occurring without a proper basis.

## **The Commissioner's Investigation**

39. Given the seriousness of its concerns in regard to the potential contraventions of the GDPR by Easylife, the ICO sent Easylife an initial investigation letter on 12 March 2021. The letter detailed the Commissioner's concerns in regard to the processing which was occurring and, in the light of the Commissioner's view that Easylife was processing special category data without a legal basis, the Commissioner also instructed Easylife to immediately stop the activity.
40. Easylife responded with an undated letter, which the Commissioner received on 1 April 2021, stating that the Health campaign had started in December 2016. It reiterated that 257,490 calls had been made, which included repeat calls and repeat sales, but did not explain how that figure correlated to the processing of data. The call figure provided by Easylife differed from the number of calls which the ICO discovered for the Health campaign through call detail records ("CDRs") obtained.
41. Easylife explained the sequence of processing as follows:

*"(i) A person buys some products from Easylife Limited in one of three ways: (i) by placing an order on line at our website [easylife.co.uk](http://easylife.co.uk), (ii) by sending by post an order form cut out from the back of one of our catalogues (see the example form annexed to this letter) or (iii) by calling our call centre and placing an order by phone.*

*(ii) The customer's personal data is entered on to our CRM system. This personal data includes the customer's contact details as well as details of their order.*

*(iii) This information is then shared with a third-party telemarketing company called [REDACTED] [REDACTED] [REDACTED] ("[REDACTED]") with whom we have a data processing agreement. It is provided to them weekly by our Data Management Company. [REDACTED] sell, on behalf of Easylife Limited, to the data provided, non-medical lifestyle beneficial products that are relevant to the customer's transactional history.*

*(iv) [REDACTED] store the data we provide to them on their secure server. They select people to call based on a multitude of factors including the date of the last order placed, frequency of making purchases, product purchased; currently and on historically and value of orders placed. They also look at a customer's transaction history to identify whether (or not) they have purchased particular products.*

*(v) The selected people are then called with a view to selling them relevant products based on the factors outlined in (iv) above."*

42. Easylife maintained that its consent statement was relevant:

*"As customers or subscribers, we will send you our catalogues and information by post or email and may telephone offering services or products such as our Health, Motor, Supercard, or Gardening*

*Clubs. If you would prefer not to receive these communications please let us know (see below) or simply unsubscribe from any of the communications you receive at the time."*

43. Easylife stated that a former employee, who had previously been a [REDACTED], had advised it that the consent statement was a sufficient basis for the sales activity carried out by [REDACTED] to be compliant. Further, Easylife said that it had a vulnerable persons policy underpinning the sales calls because many customers were elderly and were "often glad to talk to someone about their medical conditions". The calls, Easylife said, were quickly terminated if there was the slightest hint of embarrassment from the customer regarding their health condition, but, as most were elderly, they welcomed the conversation.
44. Easylife informed the ICO that it had now instructed [REDACTED] to cease the processing and that in future it would stop the profiling element of the Health telephone marketing campaign and would instead telephone customers irrespective of whether or not the customer had purchased a trigger product. Further, as a result of the ICO's investigation relating to the PECR, Easylife was now screening calls against the TPS register. Easylife and [REDACTED] offered to enter into written undertakings with the ICO to confirm their new operating procedure.
45. The ICO declined the proffered undertakings.
46. The ICO's investigation revealed no evidence that Easylife had informed individuals that their data might be used for health profiling. Easylife had not informed the ICO how many individual customers it had profiled, and had simply provided call figures and stated that some of the calls had related to the sale of face masks.

47. On 12 April 2021, the ICO asked Easylife to provide a definitive number of how many individuals had been profiled during the marketing campaign specific to the sale of health supplements.
48. In an undated letter which the ICO received on 19 April 2021 Easylife explained that it had provided 428,531 individuals' data to [REDACTED] between 1 August 2019 and 19 August 2020. This data was then "reviewed and cleaned down" to 145,400 individuals' data, based on a multitude of factors including "date of the last order placed, frequency of making purchases, product purchased currently and on historical orders and value of orders placed". Easylife then stated that a total of 257,490 attempted calls were made to those individuals.
49. Given that one factor was purchase of a trigger product, the ICO considered that Easylife had profiled 145,400 individuals.
50. On 13 May 2021, the ICO wrote to inform Easylife that the investigation had concluded.
51. On 10 August 2022, the Commissioner issued Easylife with a Notice of Intent to issue a monetary penalty. The Notice related to the facts set out above, and concerned non-compliance with the GDPR by way of unlawful processing of special category data.
52. On 2 September 2022, Easylife submitted Representations ("the Representations") to the Commissioner, making a range of legal and factual arguments, accompanied by documentary evidence. The Commissioner has considered the Representations in making his final decision in this case.

## **Personal Data Involved in the Incident**

53. The data affected by this incident comprised the personal data of 145,400 individual customers of Easylife, consisting of their names and telephone numbers, and the special category data of those 145,400 individuals, consisting of health conditions which Easylife had inferred that they probably had.

## **The Contravention of Article 5(1)(a) of the GDPR**

54. The Commissioner has considered whether the facts set out above constitute a contravention of the data protection legislation.

55. For the reasons set out below, the Commissioner has taken the view from his investigation that this breach occurred as a result of serious deficiencies in the way in which Easylife collected, processed and used the personal and special category data of 145,400 individuals.

## **Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty**

56. The Commissioner has considered the factors set out in Article 83(2) of the GDPR in deciding whether to issue a penalty. For the reasons given below, he is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising his corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

**(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.**

**Nature:**

57. Easylife conducted profiling of customers which processed special category data. The Commissioner does not accept Easylife's arguments set out in the Representations that it was not processing special category data.
58. The Commissioner does not consider that the evidence supports Easylife's argument that it was selling lifestyle products and did not make or use inferences about the data subjects' health. The Commissioner has decided that the transactional data from which Easylife made and relied on inferences was special category data, which Easylife unlawfully processed. Easylife used the transactional data to infer that the customer probably had a particular health condition, to alleviate which specific products were then marketed to the data subject, in direct marketing telephone calls.
59. The Commissioner considers that his guidance on special category data properly reflects the law on the inference of special category data.
60. The recent judgment of the Court of Justice of the European Union in *OT v Vyriausioji tarnybinės etikos komisija (Case C-184/20, 1 August 2022)* confirms that the protections which the GDPR gives to data subjects' special category data, including health data, extend beyond inherently sensitive data to cover data revealing health data indirectly, following an intellectual operation involving deduction and cross-referencing.

61. Article 9 of the GDPR provides that special category data may not be processed except under specific circumstances. The only circumstances in which Easylife could have engaged in processing of special category data in the context of its Health campaign was consent. Easylife did not collect consent to process special category data, instead relying on legitimate interest. As a result, Easylife had no lawful basis to process the data and contravened Article 6 and Article 9 of the GDPR. Furthermore, the individuals were not informed that any profiling of special category data would occur and therefore the individuals could not have reasonably expected it to happen. Easylife conducted invisible processing of special category data, and, as such, Easylife did not process the data fairly, lawfully or transparently as required by Article 5(1)(a) of the GDPR.
62. In order to process this data lawfully, Easylife would have had to collect explicit consent for the profiling from the data subjects and to update its privacy policy to indicate that special category data was to be processed by consent. Easylife's omission to do this resulted in the contravention occurring and also involved a contravention of Article 13(1)(c) of the GDPR, which required Easylife to provide a data subject with a privacy notice which informs them of the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
63. The Commissioner does not accept Easylife's argument, made in the Representations, that it had the requisite consent to process special category data because it had notified customers that it would be using customers' personal data to notify them of products "that might be of interest to you." The Commissioner does not consider that any customer would have understood the privacy policy to mean that Easylife was going to process their special category data and then use it in a direct marketing

telephone campaign.

64. According to the evidence which Easylife provided during the investigation, the contravention resulted in several hundred thousand attempted marketing calls being made to individuals whom Easylife had profiled as having health conditions. These calls were intrusive in nature because they were based on health conditions which Easylife had inferred whilst not having informed the individuals that it was going to make such inferences.

**Gravity:**

65. The contravention is serious because it consisted of unlawful invisible processing of special category data and because of the distress to individuals which resulted from it.
66. Easylife's target market was older people with long-term health conditions. Individuals in that age range, who grew up in a previous era in which electronic processing of personal data did not occur, are less likely than younger individuals to have the knowledge or ability to raise a complaint about unlawful processing of their data.
67. It is not possible for the ICO to quantify the level of damage caused, because of the invisible nature of the processing by Easylife. The damage from harassment and targeting of potentially vulnerable individuals could be wide-ranging, not least financial damage.

**Number of data subjects:**

68. Easylife collected, processed and used the personal and special category data of 145,400 individuals.

**Duration:**

69. The contravention continued for over a year, between 1 August 2019 and 19 August 2020.

**(b) the intentional or negligent character of the infringement**

70. The Commissioner considers that the contraventions were negligent because Easylife appeared unaware that it was processing special category data. Nevertheless, Easylife has a poor track record of regulatory compliance, having previously been investigated by the Commissioner for data protection concerns in 2019, having entered an undertaking with Trading Standards, and having been subject to an investigation by the Commissioner into contravention of the PECR which led to his investigation into compliance with the GDPR. Therefore, the negligence underpinning the breach is severe. Easylife should have known that the breach would occur, given that it had previously completed LIAs intended to avoid such contraventions in other marketing campaigns, which explicitly referred to special category data. It appears that Easylife misapplied the LIA which had been devised for a different marketing campaign to the Health campaign and thus failed to take the opportunity to interrogate Easylife's legitimate interests in the Health campaign and to understand what steps would have been required in order to conduct the Health campaign in compliance with the GDPR.

**(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects**

71. Upon receiving notice from the Commissioner that he believed Easylife was processing special category data, Easylife agreed to stop immediately such profiling and required ██████ to stop the Health campaign in its current format, and to continue the campaign without the element of profiling. Easylife informed the Commissioner that it would work on several remedial measures, namely:

- (i) Implementation of a new Customer Relationship Management system;
- (ii) Strengthening its Service Level Agreements and contracts with data processors;
- (iii) Introducing TPS screening to comply with the PECR;
- (iv) Changing the wording of the consent statements offered to customers.

72. Although Easylife agreed to stop the profiling, the Commissioner noted that Easylife has been very reactive in its approach to compliance and only seems to make changes to its practices in order to comply with the law when failings are discovered, and changes are required, by a regulator.

**(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32**

73. Article 25 of the GDPR requires organisations to implement data protection by both design and default. Data protection by design necessitates the consideration of privacy and data protection at the design phase of any system, service, product or process (and subsequently throughout its lifecycle). Data protection by default requires organisations to ensure that they only process data necessary to achieve a specified purpose.

74. With regard to Easylife's compliance with the above article, it is the Commissioner's view that Easylife's failure to conduct a Data Protection Impact Assessment ("DPIA") is a notable failing, and that such a step may have assisted in preventing this contravention.

75. Article 32 of the GDPR requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by their processing; to include the potential impacts these risks may have on the rights and freedoms of natural persons.

76. The Commissioner does not consider that Article 32 is relevant to its failure.

**(e) any relevant previous infringements by the controller or processor**

77. Not applicable.

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

78. Easylife have co-operated reasonably with the ICO. Upon receiving the ICO's investigation department's views in regard to the contravention, Easylife sought to mitigate the risk of profiling by completely ceasing that activity. Easylife also sought to remedy its non-compliance with the PECR which was established during the ICO's investigation into the contravention of the PECR, which had led the ICO to open its investigation into contravention of the GDPR.

**(g) the categories of personal data affected by the infringement**

79. The categories of personal data affected is set out above at paragraph 52 above and include special category data relating to health.

**(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement**

80. The infringement of the GDPR by Easylife became known to the ICO during the course of the ICO's own investigation into potential contraventions of the PECR. Easylife was ignorant of the infringement until it became known to Easylife through notification by the ICO.

81. Zero complaints were made to the ICO because the contraventions

involved invisible processing about which Easylife never informed the individuals, with the consequence that the individuals could not know that processing of their personal data and their special category data was occurring without a proper basis.

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

82. Not applicable.

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

83. Not applicable.

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

84. The Commissioner has considered the following **aggravating feature** in this case:

- The aim of the Health marketing campaign was to use the unlawful processing to gain an advantage over rival businesses and sell targeted products to individuals.

85. The Commissioner took into account the following **mitigating features**:

- Easylife has informed the ICO of its intention to:
  - Implement a new Customer Relationship Management system at the cost of [REDACTED].
  - Strengthen its Service Level Agreements and contracts with data processors.

### **Summary and Penalty**

86. For the reasons set out above, the Commissioner has decided to impose a financial penalty on Easylife. Taken together the findings above concerning the infringement, its likely impact, and the fact that Easylife failed to comply with its GDPR obligations, the Commissioner has decided to apply an effective, dissuasive and proportionate penalty reflecting the seriousness of the breach which has occurred.

### **Calculation of Penalty**

87. The Commissioner considers that imposition of a financial penalty would be an effective and proportionate action to ensure future compliance, given that previous informal action has failed. A financial penalty would be dissuasive not only to Easylife but to the whole mail order catalogue industry.

88. The Commissioner considered that the appropriate penalty amount may be up to 4% of worldwide annual turnover.

89. Following the Five Step process set out in the RAP the calculation of the penalty is as follows.
90. Step 1: An initial element removing any financial gain from the breach.  
The Commissioner has decided to impose an administrative fine on Easylife because a large number of data subjects (145,400) have been affected; the incident involves special category data; there has been repeated or wilful misconduct or serious failures to take appropriate steps to protect personal data; there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach; and it is highly likely that Easylife has benefited from a financial gain by committing the contravention.
91. The Commissioner was unable to initially identify or calculate any financial gain which Easylife may have made from its contravention of the GDPR, and proceeded to determine the provisional penalty figure without imposing an initial element to remove any financial gain from the breach.
92. The Commissioner has carefully considered the Representations made by Easylife on the level of the financial penalty. In particular, the Commissioner has noted that Easylife has calculated that it made a profit of [REDACTED] during the relevant period from the activities of [REDACTED] in the Health telemarketing campaign. The Commissioner acknowledges this disclosure, but does not amend his provisional decision not to impose an initial penalty amount removing any financial gain.
93. Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section

155(2)-(4) DPA. This refers to and repeats the matters listed in Article 83(1) and (2) as set out above.

94. The details are set out above and take into account: (a) the matters set out above at paragraphs 54 – 85, (b) the matters referred to in this section, and (c) the need to apply an effective proportionate and dissuasive fine.
95. Considering the nature, gravity, and duration of the failure, the Commissioner finds that this breach involved the processing of special category data of 145,400 individuals who were profiled for inferred health conditions. The gravity includes the impact on elderly, potentially vulnerable people, some with long-term health conditions. Easylife conducted invisible processing, with assumptions being made about health conditions based on purchased goods. The Commissioner is concerned about the on-going potential impact with regards to those individuals who may not be aware this is happening as they have not been adequately informed. The duration of the failure covered 12 months.
96. The Commissioner considers that a penalty of £750,000 would be an appropriate starting point for its consideration under Step 2, before further adjustment within Step 2 and before adjustment in accordance with Steps 3-5 below.
97. In light of the negligence of Easylife in omitting to obtain explicit consent to process the special category data, and given its attendance at a previous compliance meeting, the Commissioner considers it appropriate to increase the penalty starting point by £50,000 to £800,000.

98. He then considers it appropriate to decrease the penalty by £50,000 to £750,000 because of the action taken by Easylife to mitigate the damage or distress caused, specifically that Easylife has implemented a £200,000 CRM system, introduced improved SLAs and contracts with data processors, and worked on improving consent statements. Easylife has also stated to the Commissioner that it has ceased the practice of profiling individuals.
99. The Commissioner increases the penalty by £100,000 to £850,000 because of Easylife's responsibility taking into account technical and organisational measures which it should have implemented. Easylife conducted no data protection impact assessments as it should have done under Article 25 of the GDPR. Easylife instead relied on legitimate interests, misapplying an analysis which it had done in the past for a different marketing campaign which did not involve profiling.
100. The Commissioner has gone on to consider the following relevant factors but does not consider in this case that they should result in a change to the figure of £850,000:
- any relevant previous failures by the controller or processor;
  - the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;
  - the categories of personal data affected by the failure;
  - the manner in which the infringement became known to

the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

- the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;
- adherence to approved codes of conduct or certification mechanisms;
- any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly).

101. The Commissioner has then gone on to consider whether the penalty amount of £850,000 would be effective, proportionate, and dissuasive.

102. The Commissioner considers that available accounts include accounts up to the period ending 31 December 2020 and show a turnover of £51,631,296. These accounts were filed at Companies House on 6 October 2021. The next accounts due are scheduled to be filed by 29 December 2022.

103. The Commissioner has considered the financial documentation provided with the Representations from Easylife. In particular, he has considered the draft accounts for the year to December 2021, the management accounts for the first six months of 2022 and the administration documents concerning a key supplier of Easylife. The Commissioner also

considered Easylife's arguments that it had an exceptionally profitable year in 2020 due the pandemic. The Commissioner noted that Easylife estimated turnover of around £26,000,000 for the year to December 2022, which would be likely to incur a substantial loss, perhaps in excess of £2,000,000, and Easylife had concerns about increases in inflation, transportation costs, overheads and national insurance. The Commissioner also took account of an historic disputed claim against Easylife from a debtor in administration, which may still be payable by Easylife.

104. On the basis of the available information, the Commissioner does not consider that a penalty of £850,000 would be effective, proportionate or dissuasive and accordingly increases the penalty by £500,000 to £1,350,000.
105. This amount is considered appropriate to reflect the seriousness of the breach and takes into account in particular the need for the penalty to be effective, proportionate and dissuasive.
106. Step 3: Adding in an element to reflect any aggravating factors. Following his consideration of the aggravating factors set out above, the Commissioner considers no further aggravating factors had a material impact on the severity of the contravention and so does not increase the penalty amount from £1,350,000 at this step.
107. Step 4: Adding an amount for deterrent effect to others. The Commissioner considers that this requirement has already been addressed at Step 2, and accordingly does not propose to increase the penalty at this step.

108. Step 5: Reducing the amount to reflect any mitigating factors including ability to pay. The Commissioner considered the most recently available financial evidence at Step 2. Easylife was also invited to provide financial evidence in representations. The Commissioner has taken account of the Representations received from Easylife on 2 September 2022 in regard to ability to pay a monetary penalty at Step 2. After considering all the evidence concerning Easylife's ability to pay, the Commissioner concluded that £1,350,000 remained an appropriate penalty amount.

### **The amount of the penalty**

109. For the reasons explained above, the Commissioner is satisfied that the conditions from the factors set out in Article 83(2) of the GDPR have been met in this case and that he has adopted fair procedure. The latter has included the issuing of a Notice of Intent, in which the Commissioner set out his preliminary thinking. In reaching his final view, the Commissioner has taken into account the Representations made by Easylife on this matter.

110. In making his decision, the Commissioner has also had regard to the factors set out in s108(2)(b) of the Deregulation Act 2015; including: the nature and level of risks associated with non-compliance, including the risks to economic growth; the steps taken by the business to achieve compliance and reasons for its failure; the willingness and ability of the business to address non-compliance; the likely impact of the proposed intervention on the business, and the likely impact of the proposed intervention on the wider business community, both in terms of deterring non-compliance and economic benefits to legitimate businesses.

111. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on Easylife Limited of **£1,350,000 (one million, three hundred and fifty thousand pounds)**.

## **Conclusion**

112. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **4 November 2022** at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

113. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

- (a) The imposition of the penalty; and/or,
- (b) The amount of the penalty specified in the penalty notice

114. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

115. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired

116. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

117. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA 2018.

Dated the 4<sup>th</sup> day of October 2022.

Andy Curry  
Head of Investigations  
Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

## **ANNEX 1**

### **Rights of appeal against decisions of the Commissioner**

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.
  
2. If you decide to appeal and if the Tribunal considers:-
  - a) that the notice against which the appeal is brought is not in accordance with the law; or
  
  - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.
  
3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals  
PO Box 9300  
Arnhem House  
31 Waterloo Way  
Leicester  
LE1 8DJ

Telephone: 0203 936 8963  
Email: [grc@justice.gov.uk](mailto:grc@justice.gov.uk)

- a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.
  - b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.
4. The notice of appeal should state:-
- a) your name and address/name and address of your representative (if any);
  - b) an address where documents may be sent or delivered to you;
  - c) the name and address of the Information Commissioner;
  - d) details of the decision to which the proceedings relate;
  - e) the result that you are seeking;
  - f) the grounds on which you rely;
  - g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;
  - h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.
  
6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20))