

JUDGMENT



CLAIMANT

**Mr. Horatio Munk
Kleinestraat 1
Nijmegen
The Netherlands**

[RESPONDENT]

**The Star Maker Insurance
Grotestraat 1
Amsterdam
The Netherlands**



TABLE OF CONTENTS

A. **FACTUAL BACKGROUND** 2

B. **THE DISPUTE** 2

C. **THE ISSUES IN DISPUTE**..... 3

D. **RESPONDENT DOES NOT QUALIFY AS A “PROVIDER” WITHIN THE MEANING OF ARTICLE 52 OF THE AI ACT, AND THEREFORE CANNOT VIOLATE THE TRANSPARENCY OBLIGATION SET FORTH IN SAID PROVISION**..... 3

E. **RESPONDENT VIOLATED THE GDPR BY NOT COMPLYING WITH THE “LAWFULNESS, FAIRNESS AND TRANSPARENCY”, “PURPOSE LIMITATION” AND “DATA MINIMISATION” PRINCIPLES**..... 7

F. **RESPONDENT ACTED UNLAWFULLY BY MANIPULATING CLAIMANT’S BEHAVIOUR** ..12

G. **CLAIMANT IS ENTITLED TO COMPENSATION**14

H. **CONCLUSIONS**17



A. FACTUAL BACKGROUND

1. CLAIMANT, a Dutch resident, had planned a holiday ski trip of one week in the French Alps, to be started on 16 January 2021. On the day before his departure (15 January 2021), CLAIMANT discovered a new French law demanding insurance for civil liability and personal accidents for all holiday skiers. In light of his recent discovery, CLAIMANT immediately started to research insurers. CLAIMANT was drawn to the first insurance comparison website proposed by Google. By clicking on a hyperlink, CLAIMANT was directed to the application of RESPONDENT. After downloading and installing the application on his smartphone, CLAIMANT chose to “log in with Google”. CLAIMANT accepted the request of the app to access the data of his Google Calendar, where there were details of the scheduled ski trip. Afterwards, CLAIMANT consented to install the app, which gave RESPONDENT access to the following information about the CLAIMANT: model and battery level of the smartphone, and all the data produced by the smartphone’s motion sensors.
2. CLAIMANT selected the option “chat to us live” on the app, immediately starting a conversation with “Paulo”, a chatbot. When CLAIMANT displayed interest in civil liability and personal accidents insurance, starting from the following day for one week, “Paulo” already demonstrated knowledge of the ski holiday, and presented insurance packages for winter sports.
3. The chat was interrupted in CLAIMANT’s smartphone by a push notification about his low level of battery and estimated battery life (“Battery level: 4%. Estimated battery life: 15 minutes”). When CLAIMANT opened the app to continue the chat, the motion sensor of the smartphone detected a faster typing pace. RESPONDENT promptly made the offer with a hyperlink where CLAIMANT could view the contractual details and accept them. The offer, however, would expire in 15 minutes, with no guarantee that the contractual conditions would remain the same, if a new chat was initiated. CLAIMANT clicked on the link, accepting the offer.

B. THE DISPUTE

4. After coming back from his holiday trip, on 1 March 2021, CLAIMANT sent a letter to RESPONDENT, listing RESPONDENT’s allegedly unlawful acts. More specifically, CLAIMANT argued that RESPONDENT acted unlawfully, by (i) failing to disclose that Paulo was a chatbot, and not a human, in violation of the European AI



Act; (ii) processing CLAIMANT's data which were not relevant and limited to what was necessary for the conclusion of an insurance contract, in violation of the General Data Protection Regulation (GDPR); (iii) unfairly manipulating CLAIMANT's behaviour by pressuring him to accept the offer with techniques beyond CLAIMANT's consciousness, in violation of the AI Act and/or of EU consumer law (as implemented in Dutch national legislation, where applicable).

5. On the basis of these claims, CLAIMANT argued that it suffered stress and psychological discomfort, and requested RESPONDENT to compensate the damage arising out of this unlawful behaviour, in the amount of €5,000.00.
6. On 14 April 2021, RESPONDENT contested all the allegations against it, denying the unlawful behaviour and arguing that the CLAIMANT freely decided to conclude the contract, without any manipulation. RESPONDENT also pointed that the CLAIMANT benefited from the insurance coverage during the trip.
7. On 2 November 2021, the CLAIMANT started the present proceeding, insisting to receive compensation in the amount of €5,000.00, or a different amount to be determined by this Court.

C. THE ISSUES IN DISPUTE

8. In the light of the above, the Court ordered the parties to exchange written and oral defences on the following four issues: (i.) Has RESPONDENT violated a legal obligation to inform CLAIMANT that RESPONDENT made use of an AI system within the chat function of its app? (ii.) Has RESPONDENT violated the GDPR by processing CLAIMANT's data which were not relevant and limited to what is necessary for the conclusion of an insurance contract? (iii.) Has RESPONDENT acted unlawfully by manipulating CLAIMANT's behaviour? (iv.) Has CLAIMANT suffered a damage and, if yes, what is the amount of the compensation? These four issues will be discussed and adjudicated in turn, in the remainder of the present judgment.

D. RESPONDENT DOES NOT QUALIFY AS A "PROVIDER" WITHIN THE MEANING OF ARTICLE 52 OF THE AI ACT, AND THEREFORE CANNOT



VIOLATE THE TRANSPARENCY OBLIGATION SET FORTH IN SAID PROVISION

9. CLAIMANT argued that RESPONDENT acted unlawfully, by failing to disclose that Paulo was a chatbot, and not a human, in violation of the European AI Act.
10. RESPONDENT argued that CLAIMANT has been informed that Paulo was a chatbot, and that this was obvious from the circumstances of the conversation.
11. RESPONDENT argued that the AI act does however only impose a transparency obligation on ‘providers’, i.e. the developers of AI systems. RESPONDENT, however, is not a ‘provider’, but a ‘user’ within the meaning of the AI Act. For RESPONDENT has not developed the AI on which Paulo was based. The AI is based on GPT-3: an API to an AI text-generation system. RESPONDENT has configured the system, so to use GPT-3 as a chatbot withing its app.
12. Article 52(1) AI Act states the following: *Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.*
13. The parties are in disagreement as to the nuance of the first half of the article. The first question is whether chatbot Paulo is an AI system under the AI Act.
14. Article 3(1) AI Act states: *‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.*
15. Chatbot Paulo is a software, an API, named GPT-3, developed by OpenAI. GPT-3 is made through and uses deep learning (as stated in annex 1 AI Act: deep learning is one of many types of an AI system under 3(1) AI Act) to produce human-like text, mainly used for chatbots. GPT-s is an API which developers, who use the API, can program to their own needs which RESPONDENT so states it did. In conclusion:



GPT-3 is an artificial intelligence system under article 3(1) in combination with annex 1 AI Act.

16. The second question is whether CLAIMANT was informed that Paulo was a chatbot and not a human.
17. Article 52(1) AI Act states: *Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.*
18. The chatbot Paulo is intended to interact with natural persons (i.e. CLAIMANT). Paulo is intended to chat/interact with RESPONDENT customers. CLAIMANT states that RESPONDENT did not disclose that Paulo was a chatbot, which RESPONDENT objects, as it was also obvious from the correspondence between Paulo and CLAIMANT. From the conversations is not clear that CLAIMANT was talking to a chatbot. When CLAIMANT entered the app and saw ‘chat to us live’ there was no need for CLAIMANT to think he was not about to talk to a natural person. There is however a note on Paulo’s message “Hello! I am Paulo from Star Maker Insurance. I am available 24/7 to answer all of your questions!”. 24/7 could imply a non-human interaction. This, however, does not weigh against the humanlike interaction between CLAIMANT and the chatbot based on the GPT-3 API, in which GPT-3 stands out. As seen below.

Paulo: Hello! I am Paulo from Star Maker Insurance. I am available 24/7 to answer all of your questions!

Horatio Munk: I need a civil liability and personal accidents insurance.

Paulo: Sure! For what period do you need the insurance?

Horatio Munk: Starting from tomorrow, for a week.

Paulo: I see you have planned a ski holiday. We do offer insurance packages for winter sports.

Horatio Munk: Are you still there?

Paulo: Yes. No stress – Paulo never leaves this app! I can offer international insurance coverage for a week of winter sports, starting from tomorrow. You can view the details and accept the offer at this link. However, this offer is only valid for 15 minutes. If the



time-limit expires, open a new chat with Paulo. We cannot guarantee that the same contractual conditions will be available. It was great to chat with you! You can access, review, download and/or delete the chat log here.

19. In the light of article 52(1), AI Act RESPONDENT did not only fail to inform CLAIMANT that the chat was with a chatbot. RESPONDENT also failed to make it obvious from the circumstances and the context of use. CLAIMANT was under the impression that the correspondence was between two humans.
20. The last question to be answered is whether RESPONDENT is a ‘provider’ or ‘user’ within the meaning of the AI Act. Article 3(2) AI Act states: *‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.*
21. Based on the above, RESPONDENT argues it is not a ‘provider’ within the meaning of the AI Act. This is, in the light of the AI Act, no error in law. RESPONDENT did not develop an AI system; it merely configured the AI system made by OpenAI. The Court follows this argument.
22. RESPONDENT argues it is a user within the meaning of the AI Act. Article 3(4) AI Act states: *‘user’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.* As stated before. RESPONDENT argues it did not develop the AI on which Paulo was based. And merely configured the GPT-3 API system as to use the chatbot within its app. The Court follows this argument as it does not show an error in law. RESPONDENT is a user under article 3(4) AI Act.
23. A user has no transparency obligation under article 52(1) AI Act, only the provider. Thus, CLAIMANT’s argument fails as RESPONDENT did not act unlawfully towards CLAIMANT, since they are to be seen as a user and not a provider under article 3(2) and 3(4) AI Act.



E. RESPONDENT VIOLATED THE GDPR BY NOT COMPLYING WITH THE “LAWFULNESS, FAIRNESS AND TRANSPARENCY”, “PURPOSE LIMITATION” AND “DATA MINIMISATION” PRINCIPLES

24. CLAIMANT argues that RESPONDENT breached the General Data Protection Regulation (“GDPR”) when negotiating an insurance contract, entered into for CLAIMANT’s winter holidays. CLAIMANT alleges that some personal data that was processed by the RESPONDENT was not necessary for the conclusion of the insurance contract. In such regard, the Court’s findings are as follows.

Legal basis for the processing of CLAIMANT’s personal data

25. CLAIMANT downloaded an app developed by RESPONDENT (hereinafter, the “app”) which processed personal data of the CLAIMANT at two different moments: (i) when CLAIMANT consented to install the app; and (ii) when CLAIMANT chose the option to ‘login with Google’ in the app.

26. As shown under Article 4(11) of GDPR, consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. In this regard, from the informed facts and allegations from the Parties, the Court understands that CLAIMANT provided consent to the processing of his personal data for one specific purpose (entering into an insurance contract).

27. Therefore, the Court finds that there is sufficient legal basis for the personal data processing of CLAIMANT by RESPONDENT as defined by the GDPR, considering that consent provided by CLAIMANT for data collection when downloading the app is in line with Articles 6(1)(a) and 4(11) of the abovementioned regulation.

Principles relating to the processing of CLAIMANT’s personal data

28. Among other arguments, CLAIMANT has stated that RESPONDENT violated the GDPR by processing CLAIMANT’s personal data which were not relevant and not limited to what was necessary for the conclusion of an insurance contract. RESPONDENT objected to this argument, stating that all of the used data was relevant and necessary for the insurance contract.



29. From the facts, the Court understands that the following personal data of CLAIMANT were processed by the RESPONDENT through the app while the insurance contract was being negotiated by the parties: (i) Google Calendar information; (ii) model of the smartphone on which the app was installed; (iii) battery level of the smartphone; and (iv) data produced by the smartphone's motion sensors ("ii", "iii" and "iv", collectively hereinafter "Other Data").
30. In this regard, Article 5(1) of GDPR states that "Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (...); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (...); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Such quoted subsections are specific principles of GDPR known as "lawfulness, fairness and transparency", "purpose limitation" and "data minimisation". This being said, the Court will analyse if the RESPONDENT breached these principles related to processing of personal data when collecting CLAIMANT's information, pursuant to the GDPR rules.

Lawfulness, fairness and transparency

31. In order to reach a thorough conclusion, it is central to understand whether the "lawfulness, fairness and transparency" principle was respected or not by RESPONDENT when collecting CLAIMANT's information. For such purpose, it is necessary to differentiate between the different types of personal data collected by RESPONDENT from CLAIMANT. On the one hand, the Court will review the personal data collected from CLAIMANT's Google Calendar and, on the other hand, CLAIMANT's Other Data.
32. Regarding the data processed in CLAIMANT's Google Calendar, RESPONDENT complied with Article 6(1) of GDPR, considering that the CLAIMANT provided express consent to share information included under this calendar when logging into the app with his personal Google username and password (Article 6(1)(a)). It is important to outline that it was CLAIMANT's choice to login with his Google account into the App (being expressly informed that information from Google Calendar would be accessed by such app). In this regard, as CLAIMANT provided access to the app so that data would be retrieved from his Google Calendar, is not possible for CLAIMANT to allege that he was unaware of such data processing by



RESPONDENT. This being said, the principle of lawfulness, fairness and transparency was not breached by the RESPONDENT when processing CLAIMANT's personal data.

33. However, in connection with the Other Data, it cannot be assured that such personal information was collected lawfully and in a transparent manner. None of the events listed under subsections from (a) to (f) in Article 6(1) of GDPR were complied with by RESPONDENT when processing CLAIMANT's personal data. Then, collection of the Other Data would not be in line with the lawfulness, fairness and transparency principle.
34. Furthermore, even assuming that CLAIMANT expressly accepted sharing the Other Data with RESPONDENT through the app, CLAIMANT's acceptance would not necessarily qualify as actual consent under the GDPR. Pursuant to Article 7(4) GDPR, in case personal data that is not necessary for the performance of the contract is requested as a condition "sine qua non" to enter into the contract, such consent would not be considered as "freely" provided. This being said, in case "Other Data" was: (i) construed as non-necessary information in connection with the insurance policy (which will be reviewed below); and (ii) its consent was a necessary step to enter into the contract; acceptance provided by CLAIMANT would still not qualify as actual consent pursuant to Article 4(11) of GDPR.

Purpose limitation

35. Following the abovementioned differentiation between the Google Calendar and the Other Data for our analysis, the Court finds that personal data processed under the Google Calendar has a specified, explicit and legitimate purpose. Such conclusion derives from the fact that information included in CLAIMANT's Google Calendar is relevant and directly linked with the insurance coverage detailed in the contract. Personal data obtained from CLAIMANT's Google Calendar provides specific information that helps determine certain contractual details such as period of coverage, type of policy, risks to be covered, among others. In this sense, processing information about the trip was a necessary condition to assess CLAIMANT's situation and, subsequently, to conclude the insurance contract (Article 6(1)(b) GDPR). Therefore, it is unquestionable that such information was collected with a clear purpose directly connected with the performance of the contract.



36. However, the processing of Other Data (i.e., CLAIMANT's model of smartphone, battery usage and motion sensors) are irrelevant to the negotiation and performance of an insurance contract. In this sense, RESPONDENT's usage of this personal information was non-related with the ultimate purpose of the digital conversation in the chat box, considering that the Other Data has no link with the negotiation and performance of an insurance policy. For this reason, the Court finds that such data processing had other purposes than collecting information to arrange a proper insurance policy.
37. What is more, RESPONDENT may have employed the Other Data in an abusive way, for its own benefit and to CLAIMANT's prejudice. RESPONDENT having access to CLAIMANT's smartphone battery level and motion sensors –while talking through the chat box– could provide additional information to force the contract negotiation in favour of RESPONDENT. For instance, it could be inferred that RESPONDENT proposed a 15-minute limited offer to CLAIMANT, after: (i) acknowledging that CLAIMANT's mobile battery was low (4%); and (ii) detecting a quicker typing pace through CLAIMANT's motion sensors, which could constitute a stress symptom. Under this hypothetical scenario, it is clear how dangerous it could be to allow data processors to use personal information of consumers in abusive manners. This, in turn, raises doubts as to whether the contract negotiation was agreed freely by the Parties, or whether RESPONDENT's dominant position (caused by RESPONDENT's abusive data processing) led to a manipulation of CLAIMANT's decision-making.
38. In conclusion, even though the purpose of the personal data processing was specific, explicit and legitimate (conclusion of an insurance contract), there are sufficient grounds to conclude that the collection of Other Data was not limited to what is necessary for the abovementioned purpose. Therefore, the RESPONDENT breached the “purpose limitation” principle.

Data minimisation

39. The central aspect of the claim raised by CLAIMANT is whether the processed personal data was relevant and limited to what is necessary for the conclusion of the insurance contract. As a preliminary comment, it shall be mentioned that the terms “adequate, relevant and limited” are not specifically defined under the Article 5(1)(c) of GDPR. However, it is accurate to state that the assessment of this principle is based on what personal data is necessary to the purposes for processing. This being said, to



be in line with the GDPR, RESPONDENT shall only process personal data strictly needed to achieve the purpose of concluding the insurance contract, and not any other data that is not directly linked with such a purpose.

40. In line with the purpose limitation principle, it can be said that the data processed in the Google Calendar was adequate, relevant and limited to what is necessary in relation to the performance of the insurance contract.
41. However, the collection of the Other Data does not comply with this principle, not being adequate, relevant nor necessary for deciding the correct insurance policy for the CLAIMANT. Recital no. 50 of the GDPR states that “The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected”. Nonetheless, it is not possible to trace a link between the CLAIMANT’s smartphone model, battery life or motions sensors and the actual planning or negotiation of an insurance coverage. In this regard, RESPONDENT’s allegations that these personal data were relevant to customize the contractual offer, cannot be sustained.
42. Therefore, once again, the RESPONDENT breached the data minimisation principle when processing the Other Data.
43. In conclusion, after analysing the facts in light of GDPR provisions, together with the corresponding arguments filed by the Parties in these proceedings, there are sufficient grounds to state that the RESPONDENT did not comply with the “lawfulness, fairness and transparency”, “purpose limitation” and “data minimisation” principles.
44. On the one hand, it must be clarified that all processed data under the Google Calendar information would be in line with the abovementioned principles, according to our opinion. On the other hand, a GDPR breach would result as a consequence of the processing of the Other Data. In short, processing of the Other Data was: (i) not previously communicated in a transparent manner to CLAIMANT; (ii) not directly linked with the final purpose; and (iii) information that exceeded the scope of CLAIMANT’s personal data needed by RESPONDENT to provide a correct assessment regarding the insurance coverage.
45. This being said, the Court finds that RESPONDENT breached the aforementioned GDPR provisions.



F. RESPONDENT ACTED UNLAWFULLY BY MANIPULATING CLAIMANT'S BEHAVIOUR

46. The AI Act, a Regulation based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), aims to improve the functioning of the internal market by prohibiting – among other things – the manipulative behaviour resulting from the use of Artificial Intelligence. Recital 15 of this instrument is assertive in affirming that technology can be misused, providing tools for manipulative, exploitative, and social control practices. It also highlights how these practices disrespect values of the European Union, such as human dignity, freedom, equality, democracy, and fundamental rights of non-discrimination, data protection, and privacy. Article 5(1)(a) specifically prohibits the use of AI systems that utilize subliminal techniques beyond a person's consciousness to distort their behaviour and cause physical or psychological harm. Applying the provision to the case, CLAIMANT was not aware of the techniques utilized by RESPONDENT, meaning that he did not know that the battery level of his phone or his typing pace could affect the time-limit of the offer, in order to generate a sense of urgency and the inclination to take impulsive decisions. Considering these facts, it is clear how RESPONDENT used the data to manipulate the CLAIMANT's behaviour, which is a violation of the AI Act.
47. The UCPD is also pertinent to the case. Recital 7 points out the application of the Directive to commercial practices that influences consumers' decisions, on business-to-consumer commercial practices, without prejudice of contracts or other regulations (article 3). Article 5 UCPD determines that a practice is considered unfair "if it is contrary to the requirements of professional diligence and it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer (...)". CLAIMANT had his decision influenced by the behaviour of the DEFENDANT, who used the collected data to provide an "exclusive" offer, with validity expiration pairing the battery life of the CLAIMANT's smartphone. This practice fits the Article 6 definition of a misleading action, when the DEFENDANT made an offer that, although it might be factually correct, influenced CLAIMANT's transactional decision to accept the offer without further consideration or contractual analysis. It is not enough to highlight that the limited time offer pairing with the smartphone battery level is a strong indication of the use of data to influence the



behaviour, considering that the CLAIMANT would miss the supposedly advantageous offer if the battery ended.

48. Through Artificial Intelligence embedded in an application, a company can access the personal data of its customers, such as motion sensors and battery levels, under the excuse of enhancing the customer's experience. However, most of the time, the customers are not acquainted with the purpose for what this information is being collected, or even that it is being collected. Moreover, contrary to the W3C recommendations, these companies often use the data to track the customer's behaviour and make decisions from it. After experiments, specialists acknowledged that the current tracking-block applications only successfully block an insignificant portion of the scripts accessing the smartphone's sensors. Although CLAIMANT consented to the application accessing the motion sensors and battery life of his phone, he was not aware of the purpose, nor that his behaviour affected the ongoing chat. There is no doubt that the RESPONDENT accessed CLAIMANT's data with a tracking purpose, resulting in an offer limited to the remaining battery life.
49. Beyond that, companies are explicitly using marketing strategies that cause emotional triggers in the customers to increase their sales. The most common methods are the time-limited and personalized offers, which can create a sense of urgency and the anxious idea that the customer must act fast to secure the best deal. The DEFENDANT clearly made use of these strategies when creating an offer that would expire in 15 minutes, after which there was no guarantee of the same benefits. Under this induced pressure, CLAIMANT felt compelled to accept the offer, without a deep analysis of the insurance policy or even the price.
50. RESPONDENT violated several provisions of the AI Act and the Unfair Commercial Practices Directive (as implemented in Dutch law). Related to the former, RESPONDENT utilized subliminal techniques to distort the CLAIMANT's behaviour, beyond his consciousness, which specifically violates the prohibition embedded in article 5(1)(a) AI Act. Additionally, RESPONDENT infringed article 6 of the UCPD (as implemented in Dutch law) when it provided information that was likely to cause a transactional decision that CLAIMANT would not have been taken otherwise, which amounts to a misleading action.
51. It is evident that traders and consumers have a disparity of resources, which requires measures to rebalance their position in court. In observance of this rule, it would be an



extreme burden if CLAIMANT had to prove the causal link between data collected by RESPONDENT and the details of the offer formulated by the chatbot.

52. It is clear from the factual evidence that RESPONDENT used subliminal technics to distort the CLAIMANT's behaviour, by collecting his data and manipulating his decisions. Therefore, the Court finds that RESPONDENT has violated the AI Act as well as the national provisions implementing the UCPD.

G. CLAIMANT IS ENTITLED TO COMPENSATION

53. A way to claim damages in Dutch Civil Law is via article 6:162 Dutch Civil Code (DCC). This article states that the one who commits an unlawful act towards someone else is obliged to compensate the damage suffered because of that act. To get some compensation for damage, there has to be an assessment whether the requirements of this article are met. Furthermore the GDPR and the AI act shall play a role in determining whether the requirements of article 6:162 Dutch Civil Code are met.
54. This judgment will mostly focus on whether there is any compensable damage. The definition of damages in the DCC can be found in article 6:95 DCC, read together with article 6:106 DCC. Damage that must be compensated can be financial loss, or any other loss for as far as the law gives one the right for compensation. Then article 6:106 specifies what 'other loss' can be – for damages that are not financial loss, the injured party has the right for fair compensation in the cases when: (a) The person responsible intended to cause such damage; or (b) the injured party has suffered physical injury, has been harmed in his honor, or reputation, or has been otherwise damaged. The provision also mentions another option, which is however not applicable to the case at hand, and will therefore not be discussed further.
55. In Dutch Civil Law, it is rarely the case that immaterial damages are compensated. The unlawful processing of data will often only have an immaterial impact, such as frustration, tension, uncertainty and some other negative emotions. This does not automatically qualify as relevant damage.
56. In the *EBI* case, the Dutch Supreme Court created a formula based on which the injured party can have a right to compensation of immaterial damage, if the nature and seriousness of the violation and the consequences are of such a level that it constitutes a damage within the meaning of article 6:106 §1, subsection b, DCC, namely



‘otherwise damaged’.¹ Psychological damage is not the main factor in this category, and the damage does not necessarily have to result from a violation of a fundamental right. In relevant literature, this subcategory is also named the ‘residual category’.

57. From the *EBI* case follows a main rule, and an exception. The main rule is that the injured party has to support their claim that there has been a violation, and that there were consequences, and that those fall under the ‘residual category’. Ways to prove immaterial damages can be documentation by medical specialists, or from people out of the personal environment of the injured party. The exception is that the injured party does not have to give any concrete proof of detrimental consequences, when the nature and seriousness of the violation are of such a level that those consequences could have been expected.
58. However, Dutch courts are also obliged to ensure that EU law has full effect.² Amongst other things, this means that they must interpret national law in such way that the objectives of the relevant EU law are achieved.³ Article 82 GDPR gives the injured party the right to pursue for compensation for immaterial damage, resulting from an infringement of the Regulation. ‘Damage’ in this article must be interpreted in an autonomous way. This means that the judge must interpret damage in the context of the Regulation, and the goals and rights it wants to protect.⁴ The goals of the GDPR thus give an interpretation of the concept of damage. The first goal is control over the personal data by the data subject, which could mean that the principles of the GDPR are completely complied with by the data controller.⁵ Therefore, the principles mentioned in article 5 §1 GDPR must be complied with: lawfulness, transparency, relation to a defined purpose, data minimization, accurateness and insurance of appropriate security. An infringement of the GDPR can mean that there is a loss of that control, which in turn can be a ground for compensation.

¹ HR 19 March 2019, ECLI:NL:HR:2019:376, NJ 2019/162 (*EBI*).

² CJEU 19 June 1990, C-213/89 (*Factortame e.a.*); CJEU 19 November 1991, C-6/90 and C-9/90 (*Francovich*); CJEU 20 September 2001, C-453/99 (*Courage/Crehan*); CJEU 19 July 2006 C-295/04 and C-298/04 (*Manfredi*).

³ CJEU 10 April 1984, 14/83 (*Von Colson and Kamann*); CJEU 13 November 1990, C-106/89 (*Marleasing*); CJEU 26 September 2000, C-262/97 (*Engelbrecht*); CJEU 7 January 2004, C-60/02 (*Rolex e.a.*).

⁴ T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens*, *O&R* nr. 126, 2021, §7.3.1.

⁵ Recital 146 GDPR.



59. Besides, article 82 GDPR also ensures that the GDPR is properly enforced. Enforcement is an important principle of the GDPR.⁶ However, enforcement by the supervisory authorities is not sufficient by itself; therefore, the possible enforcement via private law, by way of giving the injured party the right to sue for damages, can be important for effective enforcement of the GDPR.⁷ The Court of Justice of the European Union emphasizes that a right to compensation for damages can contribute to the full effect of EU law.⁸ In light of this, courts are under an obligation to give a broad interpretation to the definition of damage.⁹ According to literature, this is a strong indication that there is a possibility to assume damage when it is not evident, and the injured party would not have to prove the concrete consequences of the infringement.¹⁰ As a *lex specialis*, the EU definition of damage takes precedence over the national definition.
60. However, the Court of Justice of the European Union has not given an explanation of ‘compensable damage’ when there has been unlawful processing of data. From other judgments it follows that there must be actual and certain damage.¹¹ Therefore, a substantial violation of the GDPR must have taken place, so that not being able to enforce the violated norm would result in an impairment on the effectiveness of the GDPR.¹² Nevertheless, because of a lack of explanation from the Court of Justice of the European Union, the Dutch judge still has to judge partly on the basis of Dutch law.¹³
61. Under Dutch law, the amount of the compensation for immaterial damage is not high in general, unless it concerns a case of identity fraud. From recent judgments, it seems that the amount of compensation can vary from € 100 to € 1000.¹⁴ Article 82 GDPR also does not give an indication for determining immaterial damages.

⁶ Recital 7, 129 and 148 GDPR.

⁷ Walree 2021 §6.2.3; T.F. Walree, over de (on)mogelijkheden van vergoeding van immateriële schade bij de onrechtmatige verwerking van persoonsgegevens, *WNPR* 2017/7172, p. 921-930.

⁸ CJEU 20 September 2001, C-453/99 (*Courage/Crehan*); CJEU 13 July 2006, C-296/04 and C-298/04 (*Manfredi*); CJEU 5 June 2014, C-557/12 (*Kone*).

⁹ Recital 146 GDPR.

¹⁰ Walree 2021 §7.3.1.

¹¹ CJEU 4 April 2017, C-337/15 (*Europese Ombudsman*); CJEU 21 February 2008, C-348/06 (*Commission/Girardot*); CJEU 9 November 2006, C243/05 (*Agraz v Commission*).

¹² Walree 2021 §7.3.1.

¹³ Walree 2021 §6.3.

¹⁴ Walree 2021 (§7.3.2; Rb. Noord-Nederland, 3 May 2017, ECLI:NL:RBNNE:2017:1700 (*X/Advocatenkantoor*); Rb. Noord-Holland (ktr.) 28 December 2016, ECLI:NL:RBNHO:2016:10635 (*X/Van Hees*).



62. In this case, there has been an infringement of the law, but the question remains whether that infringement is of such a nature and seriousness that CLAIMANT does not need to prove the consequences, namely stress and psychological discomfort. In this case, CLAIMANT only states that he experienced these consequences, but has not furnished any proof of this, and the fact that he only states this a month and a half after the infringement has taken place, makes it seem that the consequences are not as severe as he alleges. Hence, if one were to strictly apply Dutch law, there would not be any damages. However, to ensure the effectiveness of EU law, national law must be put aside.¹⁵ As stated before, the national judge is obligated to give full effect to EU law. The context and purpose of the relevant European legislation must be taken into account. Therefore, the Court finds that there are compensable damages.
63. In case of immaterial damages, the damages must be estimated on the basis of fairness. Factors to consider, according to CLAIMANT, are:
- The nature and degree of personal harm;
 - The duration of personal harm;
 - The age of CLAIMANT;
 - The existence and level of psychological harm;
 - Other circumstances regarding CLAIMANT;
 - Other circumstances regarding RESPONDENT.
64. Taking all of this into account, the Court cannot award CLAIMANT the full € 5.000,00. The nature of the harm, as the infringement of the GDPR, is very clear and big enough to determine that there is damage that should be compensated. However, CLAIMANT has not substantiated his claims that he suffered stress and psychological discomfort to such a degree that he should be awarded more than follows from existing case law. However, a compensation that is too little will not ensure the enforcement of EU law. Therefore, the Court awards the highest possible compensation, namely € 1.000,00.

H. CONCLUSIONS

For the reasons stated above, the Court:

¹⁵ CJEU 16 December 1976, C-33/76 (*Rewe*); CJEU 10 April 1984, C-14/83 (*Van Colson*); CJEU 5 June 2014, C-557/12 (*Kone*).



- rejects CLAIMANT's claim that RESPONDENT acted unlawfully by violating Article 52 of the AI Act;
- allows CLAIMANT's claims that RESPONDENT acted unlawfully by violating Articles 5 and 6 of the GDPR, Article 5 of the AI Act, and Article 6 of the UCPD (as implemented in Dutch law);
- orders RESPONDENT to pay CLAIMANT € 1.000,00 in compensation;
- orders RESPONDENT to pay CLAIMANT the costs of the present proceedings, in the amount of € 500,00.

The judgment was rendered publicly in Nijmegen on 25 March 2022.