noyb - European Centre for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

complaint under articles 77(1), 80(1) of the data protection regulation

noyb Case no: C055

brought in by

XXX, Germany (hereinafter "the **complainant**"),

represented by

noyb - European Centre for Digital Rights, a non-profit organisation with its registered office at Goldschlagstraße 172/4/2, Vienna1140, Austria, ZVR: 1354838270 (hereinafter "***noyb***"),

against

- paydirekt GmbH, https://www.paydirekt.de/, Stephanstr. 14-16, 60313 Frankfurt am Main, Germany (hereinafter "**the responsible party**"; "**the respondent**"). The respondent operates the online payment system "paydirekt".

1 Representation

1. *noyb* is a non-profit organisation active in the field of data protection (Articles of Association, **Annex 1**). The complainant has mandated *noyb to* represent her pursuant to Article 80(1) of the GDPR (**Annex 2**).

2. Communication between *noyb* and the supervisory authority in the context of this procedure can be made by e-mail to XXX with reference to the case number mentioned in the title of this complaint.

2 Facts

3. On XXX and XXX, the complainant placed an order for various products at the online shop *delmed Versandapotheke* https://www.delmed.de/, Atida Plus B.V., Ampèrestraat Unit 7PE1,5928 Venlo, the Netherlands (hereinafter "delmed") and at the 24.01.2021online shop *Mac's Mystic Store*, https://www.mystic-store.com/, Meßinger Fashion & Brands, Marco Meßinger, Ludwig- Feuerbach-Straße Nuremberg15,90489, Germany (hereinafter "Mac's") (**Annexes 3a and 3b** and **Annexes 4a and 4b**).

4. The orders were paid for directly afterwards using the respondent's online payment service "paydirekt". paydirekt was offered as a payment method by the respective shops and was directly integrated into the check-out process.

5. The complainant has been a user of the paydirekt payment service since around 2017 and is registered there with the email address XXX. According to its own privacy policy, paydirekt is the responsible party for the data processing relevant here (see **annex16**).

6. The order at delmed in April 2020 included the following products: *AVENE Cicalfate+ Acute Care Cream*, *GUM Junior Mouthwash Strawberry*, *HYLO-COMOD Eye Drops*, *SENSODYNE ProEnamel Junior Toothpaste*.

7. The order placed with delmed in May 2020 included the following items: *LENSCARE ClearSept 380 ml+container*, *VITA POS eye ointment*, *GUM ActiVital mouth rinse*, *HYLO DUAL Intense eye drops*.

8. The order at Mac's was for the following products: *Leather Penis Ring*, *Nipple Pull Loop*, *Secura Santa's Coming Condoms*, *Anal Plug with Stimulation Ball, Jelly Fun Plug orange*, *Heavy Ball*.

9. When visiting her paydirekt online portal in April, the complainant discovered2021 that the respective purchase items of these orders had been transmitted to the respondent and were visible in the complainant's account (**Annexes 5a and 5b** and **Annex 6**).

10. The display of the purchase items on the respondent's portal surprised the complainant. This was because the items were not displayed between 2017 and the beginning of 2020. For purchases from this period, the respondent's account only shows the trader, order date and -time, order number, transaction number, customer number, value of goods, shipping costs and total amount (**Annexes 7a to 7d**).

11. Surprised by this new "feature" of the respondent, the complainant contacted the officer by email on 28.01.2021 and asked why the purchase items were sent to the respondent and why they were visible in her account (**Annex 8**).

12. On , the respondent replied28.01.2021 by email and explained that the transmission of the purchase items was solely at the discretion of the respective trader and that the items were not relevant for them (**Annex9).**

13. Also on , the complainant replied28.01.2021 to the respondent. She stated that she considered the respondent to be responsible for the processing of the posts (**annex10**).

14. On 29.01.2021, the respondent reiterated that it was not "*interested*" *in the* contents of the purchase items because they were also "*not the subject of the reported challenges*" of the respondent's customers. Therefore, the complainant should contact the trader if she wished to stop the transmission of the details (**Annex 11**).

15. 23.06.2021The data protection officer of the controller contacted the complainant by letter of (**Annexes 12a-c**). In this letter, the data protection officer explained that the processing of the shopping basket items was carried out so that (1) the user could check the correctness of the shopping basket, (2) the user could *make* use of "buyer protection" in the event of a conflict, (3) according to the general terms and conditions, the user was provided with an overview of his or her paydirekt payments and, finally, (4) because the transmission was "*customary in the market",* met the service expectations of the users and "*considerably simplified*" the processing of conflict cases.

16. Because the DPO's letter was not very enlightening, *noyb* contacted the data protection officer of the controller on behalf of the complainant on 21.06.2021. With a view to exonerating the authorities, *noyb* requested the respondent to adapt its processing activities accordingly and to carry out a deletion of the unlawfully processed personal data of the complainant by 22.07.2021 (**Annex 13**).

17. On , 02.07.2021the data protection officer replied by email: "*we have taken note of your message*".

18. On 05.07.2021, *noyb sent an* email reminder that substantive comments were expected22.07.2021 by the deadline. The deadline passed without any further comment from the controller. Therefore, *noyb* offered28.07.2021 an extension of the deadline until the date of 26.07.2021notification of a complaint pursuant to Article 80(1) of the GDPR (**Annex 14**). The deadline passed without any further feedback from the controller, which is why the present complaint has arisen.

19. On , 17.11.2021the complainant noticed the respondent's statement about the use of her personal data when she logged out of the customer portal:
"*Your data will only be processed for payment*" (**attachment15).**

20. Point 2 of the respondent's privacy policy (**Annex 16**) also states that "*paydirekt GmbH processes your data to enable paydirekt payments.* "

21. Under *point 2.3 When making payments and refunds* (own emphasis), the respondent specifies the processing for payments:

> paydirekt GmbH collects and stores the transaction data of paydirekt payments. **Transaction data are the transaction reference, the transaction ID and information on the shopping basket. Information on the shopping basket is provided to paydirekt GmbH by the merchant if the merchant supports this.** This data enables

the paydirekt GmbH and the bank a later identification of the transaction (e.g. for refunds). This makes it possible to allocate the transaction to the respective participant. paydirekt GmbH transmits transaction data to the bank if paydirekt is mapped in your online banking at the bank. Otherwise, paydirekt GmbH transmits the transaction data to the bank for the processing of refunds.

22. Transaction data will be additionally processed for *reversals* and *conflicts in* accordance with the *item In the event of2.5* reversals *or* conflicts.

23. The legal basis for the processing of transaction data is stated in *point 3. What is the legal basis for processing the data and how long will your data be stored?* the performance of the contract pursuant to Article 6(1)(b) DSGVO and the fulfilment of legal obligations pursuant to Article 6(1)(c) DSGVO.

24. What the "shopping cart information" is from a technical point of view is explained in the paydirekt documentation "REST API for merchants", currently available1.80.0 in the version. Thus, it is an array of items whose transmission is "*optional*" for the merchant. This array is described in the documentation as follows: "*The individual items of the shopping basket. It is recommended to transmit these values. This improves the detection of fraudulent transactions and helps to avoid disputes.* " The array itself consists of the fields "quantity", "name", "ean", "price", which are all required except for the field "ean" (cf**. Annex 17**, p. 14, 5329,, 57, 63, 79).

25. Finally, it should be noted that the respondent supports merchants in the integration of the payment system, inter alia, through recommended shop plug-ins, which are probably also commissionedby the

respondent:https://www.paydirekt.de/haendler/paydirekt-online-bezahlen-haendler-kunden.html.

3 Grounds of appeal

3.1 Violated rights

26. The complainant alleges the following violations of law:

- **Article 9(1) DSGVO:** The controller processes special categories of personal data with the purchasing positions at delmed and Mac's, but cannot rely on any of the permissive facts mentioned in Article 9(2) DSGVO. Therefore, there is a breach of the fundamental prohibition of processing special categories of personal data pursuant to Article 9(1) DSGVO.

- **Article 5(1)(a) GDPR:** Due to the breach of Article 9(1) of the GDPR, the controller automatically breaches the principle of lawfulness of Article 5(1)(a) of the GDPR.

- **Article 5(1)(c) of the GDPR:** Furthermore, the controller processes personal data with the purchasing positions which are not limited to what is necessary for the purposes of the processing. Thus, he violates the principle of data minimisation according to Article 5(1)(c) GDPR.

- **Article 25(1) GDPR:** By setting up its technical infrastructure to receive and process personal data that is not limited to what is necessary for the purposes of the processing, the controller is also in breach of its obligation under Article 25(1) of the GDPR to take appropriate technical and organisational measures to ensure that principles such as data minimisation are complied with.

3.2 On the infringement of Article 9(1) of the GDPR

3.2.1 Processing of special categories of personal data

27. By displaying and otherwise processing delmed's and Mac's purchasing positions in the Customer Portal, the Controller processes special categories of personal data.

28. In any case, the items *HYLO COMOD eye drops*, *HYLO DUAL Intense eye drops* and *VITA POS eye ointment* at delmed are health data because conclusions can be drawn on the basis of these data that the complainant has health complaints with her eyes and is seeking relief for this. It is irrelevant for the classification as health data whether the person responsible has an intention to evaluate the health significance of the respective data (cf. inter alia Kühling/Buchner/Weichert, 3rd ed. 2020, DS-GVO Art. 9 marginal no. 37; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 9 Rn. 11 f., beck-online).

29. In Mac's case, all of the items are personal data relating to the complainant's sex life because all of the respective purchase items reveal the nature of her sexual activities (cf. Kühling/Buchner/Weichert, 3rd ed. 2020, GDPR Art. 9 para. 42).

3.2.2 No authorisation under Article 9(2) of the GDPR

30. The controller may not rely on any of the grounds for authorisation exhaustively listed in Article 9(2) of the GDPR for the aforementioned processing operations.

31. In particular, the complainant did not give her explicit consent to the processing of the purchase positions pursuant to Article 9(2)(a) of the GDPR. Rather, the processing of the purchase items was carried out contrary to her ideas and wishes. Until she discovered the display of the purchase items in the customer portal, the complainant assumed that the controller neither receives nor processes the purchase items in the context of the use of the payment service, as was the case before the beginning, as evidenced2020 by her previous visits to the respondent's customer portal.

32. Consequently, the respondent is in breach of the prohibition on processing special categories of personal data under Article 9(1) of the GDPR.

3.3 On the breach of Article 5(1)(a) GDPR

33. In the absence of an authorisation under Article 9(2) of the GDPR for the processing of special categories of personal data in the context of shopping cart items, the controller is also in breach of the principle of lawfulness of Article 5(1)(a) of the GDPR.

3.4 On the breach of Article 5(1)(c) GDPR

34. The processing of shopping cart items as data covered by Article 9(1) of the GDPR violates the principle of data minimisation under Article 5(1)(c) of the GDPR.

35. The principle of data minimisation requires that only those data are processed that are absolutely necessary for the respective purpose. According to the data protection information of the controller, the purposes of the processing of the complainant's purchase items in the present case basically include a) the execution of the payment, b) the presentation of an overview of the payments made and, if relevant, c) the *facilitated* processing of reversals and d) cases of conflict (cf**. Annexes 12a-c** and **Annex 16**).

On "customary in the market" and the "service expectation

36. The data protection officer of the controller additionally mentions as "purposes" for the processing of the purchase items that the processing is 4) *customary in the market* and corresponds to the service expectations of the users (cf**. Annexes 12a-c**). Because the marketability and the service expectations of the users are not processing purposes per se, but motives for the processing, these two motives are irrelevant for the question of necessity in the context of data minimisation.

37. In addition, these justifications are also simply wrong: Neither in the case of transactions by credit card, bank transfer or direct debit are the individual items of an invoice transmitted to credit card companies, banks or other bodies. In addition to the final amount, payer and payee, a maximum of one payment reference is processed. Any further collection of individual purchasing behaviour is <u>not </u>customary in the market.

38. If individual customers actually wanted this service, this would be easy to map via consent. However, instead of asking the data subject for consent, paydirekt leaves the decision to the merchant - i.e. a third party.

Optional data processing contradicts necessity

39. According to the respondent's own information in its privacy statement, "shopping basket information" is only processed if the trader also transmits it to the respondent (see **Annex 16**, point 2.3). This also contradicts the alleged necessity: If the transmission of the shopping items to the merchant is
If the data is "surrendered", its processing cannot be necessary at all in order to use the paydirekt payment service.

40. Even broken down by the respective individual purposes, it is clear that the processing of the purchase items is neither necessary for a) the execution of the payment (because the sum, merchant and transaction number are sufficient for this) nor b) for the presentation of an overview.

about the payments made (because in a normal account statement one does not see the purchase items either) is necessary.

Reversal

41. Also c) Reversals can in principle be carried out without processing the purchase items. The respondent simply follows the trader's instruction to carry out a reversal without regard to the purchase items.

42. As with all other methods of payment (from cash to PayPal), the customer must receive an invoice that complies with the law and contains the detailed information that the customer needs in the event of a reversal. In those exceptional cases where the individual invoice items are actually relevant in the event of irregularities, the customer may submit these accordingly in the individual case. Storage of this data for future reference is neither necessary nor legally compliant.

43. Finally, even for d) the processing of conflict cases, the purchase items are not always relevant, e.g. because a parcel was not delivered and this can also be proven with the shipment tracking. In cases where the purchase items are relevant to the conflict, the relevant purchase items can be requested separately. Stockpiling processing in the event of a conflict, where only some of the purchase items may be necessary, does not constitute general necessity within the meaning of Article 5(1)(b) of the GDPR.

44. This lack of necessity is furthermore evident from the fact that the transmission of the purchase items is optional from a technical point of view according to the current infrastructure of the respondent. According to the paydirekt documentation "REST API for Merchants" in version 1.80.0, the field "*items"* has the property "*optional*" and is described as follows: "*The individual items of the shopping cart. It is recommended to pass these values. This improves the detection of fraudulent transactions and helps to avoid disputes.* " (cf**. Annex 17**, p. 14, 29, 53, 57, 63).

45. The fact that the data is transferred to the respondent by the trader is irrelevant here. The respondent as the controller must also comply with the principles of Article 5 of the GDPR for all data that it processes itself.

3.5 On the breach of Article 25(1) of the GDPR

46. By always processing shopping cart items submitted by merchants without distinguishing whether it has a legal basis for these personal data or complies with the principle of data minimisation, the respondent breaches its obligation under Article 25(1) of the GDPR to take technical and organisational measures to ensure that data protection principles such as data minimisation or lawfulness are effectively implemented.

47. A correct implementation of the obligation under Article 25(1) of the GDPR would be a setting option at the respondent so that the shopping cart items for traders where special categories of personal data are processed are not

are processed. This is the case, for example, with the payment service Klarna Bank AB (https://www.klarna.com/de/), which is why the statement of the respondent's data protection officer that the transmission of shopping basket items is standard market practice for merchants who process Article 9(1) GDPR data is incorrect.

48. To make matters worse, the transmission of the shopping basket items in the complainant's orders with delmed and Mac's is due to the shop plug-ins commissioned by the respondent, which these traders use or have used. The plug-ins should have the setting option not to always transmit shopping cart items, e.g. if these items represent special categories of personal data.

4 MOTIONS AND REQUESTS

1) Request for comprehensive investigation

The complainant requests the competent supervisory authority to fully investigate this complaint in accordance with the powers conferred on it under Article 58(1) GDPR, in particular to clarify the following factual elements:

(i) What measures has the respondent taken to comply with its obligations under Article 25(1) of the GDPR with regard to Article 9(1) GDPR data?

(ii) What design specifications did the respondent give up for the development of its shop plug-ins?

(iii) What data does the respondent use to send personalised advertising to the complainant (cf**. Annex 18**, where e.g. medicines and camping articles are advertised)?

2) Request for a declaration of infringement

The competent supervisory authority shall

- after identification of the specific data processing operations carried out and the purposes of such processing operations,

decide as follows:

(i) the respondent infringed Article 9(1) of the GDPR by processing the complainant's purchasing positions without a legal basis, to the extent that these positions constitute special categories of personal data.

(ii) the respondent infringed Article 5(1)(a) of the GDPR by processing the complainant's purchasing positions without a legal basis, insofar as those positions constitute special categories of personal data.

(iii) the respondent infringed Article 5(1)(c) of the GDPR by processing the complainant's purchasing positions even though they were not necessary for the processing purposes pursued.

(iv) the respondent infringed Article 25(1) of the GDPR by designing its technical and organisational measures without taking into account the principles of lawfulness and data minimisation incumbent upon it, thereby enabling and encouraging the processing of special categories of personal data.

3) Request for cancellation

The competent supervisory authority may, after having established the violations of law, order the respondent,

delete the unlawfully processed personal data of the complainant (Article 58(2)(g) in conjunction with Article 17(1)(d) GDPR).

4) Request instruction to bring processing operations into compliance with the GDPR

The complainant requests the competent supervisory authority to order the respondent to bring its processing operations into compliance with the GDPR in accordance with the identified infringements (Article 58(2)(d) GDPR).

5) Requesting the imposition of effective, proportionate and dissuasive financial penalties

Finally, the complainant suggests that an effective, proportionate and dissuasive fine be imposed on the respondent pursuant to Article 58(2)(i) in conjunction with Article 83(5)(b) of the GDPR, taking into account that, inter alia.

(i) the complainant is in all likelihood only one of potentially millions of data subjects whose special categories of personal data are unlawfully processed by the respondent (Article 83(2)(a) GDPR).

(ii) the infringement was at least negligent, if not intentional, because the prior notices and requests of both the complainant and *noybs* were superficially dismissed (Article 83(2)(b) GDPR).

(iii) the measures required under Article 25 GDPR have simply not been implemented (Article 83(2)(d) GDPR).

(iv) special categories of personal data are involved (Article 83(2)(g) GDPR).

Vienna, 25.02.2022