ÚRAD NA OCHRANU
OSOBNÝCH ÚDAJOV
SLOVENSKEJ REPUBLIKY

odbor správnych konaní
Hraničná 12, 820 07 Bratislava

National case no. 00275/2024-Os

In Bratislava, Slovakia
13.11.2024

IMI no. A56 - 327795
IMI no. CR – 332013

Official record

to discontinue the processing regarding the complaint pursuant to Sec. 100 (5) of the Act no. 18/2018 Coll. on Personal Data Protection and amending and supplementing certain Acts (hereinafter referred as „Slovak Data Protection Act")

On March 22, 2021, the Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as the "Office") received a complaint from complainant, in which he objected to the fact that on August 2, 2021 an e-mail was sent to his e-mail address from the company NaturaMed Pharmaceuticals s.r.o., with registered office in U Smaltovny 625, 370 01 České Budějovice, ID: 26106965 (hereinafter referred to as "company" or "controller" "NaturaMed Pharmaceuticals s.r.o. ") with delivered document (confirmation of product order) in the name of another data subject. He claimed that it was another natural person, while he thought that the company violated the principles of personal data processing, in particular the principle of integrity and confidentiality, as there was a security incident in connection with the protection of personal data for the order made via www. vitasolaris.sk.. He believed that the violation of personal data protection occurred because the company sent a document with the personal data of another person to the wrong e-mail address, the company also did not report the data breach incident to the supervisory authority within the statutory deadline.

The Office based on the findings of Czech supervisory authority as LSA and on the basis of the provisions of Sec. 100 (5) (a) of Slovak Data Protection Act and Art. 60 (8) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter as "GDPR"), decides to **discontinue** the complaint [national case no. 00275/2024-Os, IMI no. A56 327795, Case register 332013].

REASONING

On March 22, 2021, the Office received a complaint from complainant to initiate personal data protection proceedings against the company NaturaMed Pharmaceuticals s.r.o.based on the violation of security.

The complaint is of cross-border nature, since the controller is established in the Czech Republic and it is likely that the processing of personal data significantly affects the persons concerned in several European member states. The Office therefore requested the Czech

supervisory authority to deal with the matter in question, as it is within the meaning of Art. 56 of the GDPR entitled to investigate the matter. The Office is concerned supervisory authority for this cross-border processing. The Office and the Czech supervisory authority provided each other with relevant information and assistance in the matter in question for the sake of consistent implementation and application of the GDPR and adopted measures for effective mutual cooperation.

Pursuant to Art 4 (1) GDPR, for the purposes of this Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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.

Pursuant to Art. 4 (2) GDPR, for the purposes of this Regulation: 'processing' means 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.

Pursuant to Art. 4 (23) GDPR, for the purposes of this Regulation: 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to Art. 55 (1) of the GDPR, each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Pursuant to Art 56 (1) GDPR, without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

Pursuant to Art. 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

Úrad na ochranu osobných údajov | Hraničná 12 | 820 07 Bratislava 27 | Slovenská republika
tel.: 02/32313214 | fax: 02/32313214 | e-mail: statny.dozor@pdp.gov.sk | www.dataprotection.gov.sk

Pursuant to Art. 60(8) GDPR, by derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

Pursuant to Art. 78 (1) GDPR, without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Pursuant to Sec. 99 (1) of the Slovak Data Protection Act The purpose of personal data protection proceeding (hereafter as "proceeding") is to determine whether there was any infringement of the rights of natural persons when their personal data were processed or if there was any violation to this Act or GDPR in the area of personal data protection; and, if any deficiencies are identified, if it is reasonable and useful, to impose corrective measures or impose a fine for violation of this Act or GDPR .

Pursuant to Sec. 100 (1) of the Slovak Data Protection Act, the proceeding is initiated based on the complaint of a data subject that claims that his or her rights lay down by this Act are directly influenced (hereafter as "the complainant"), or without a complaint.

Pursuant to Sec. 100 (5) (a) of the Slovak Data Protection Act, (5) The Office shall discontinue the complaint if the complaint is manifestly unfounded.

The Czech supervisory authority has investigated the matter, while contacting the company with a request for information, in which the company was invited to comment on a complaint.

Summary and proposed procedure of the Czech supervisory authority as the lead supervisory authority for cross-border processing:

The documents "NaturaMed´s General Commercial Terms" and "Information on Processing of Personal Data by NaturaMed", published by the Company on the Slovak version of its e-shop (www.naturamed.sk), show that the controller of personal data processed in relation to the Company´s business activity on the territory of the Slovak Republic is NaturaMed Pharmaceuticals s.r.o. established in the Czech Republic. With regard to the aforementioned facts, the Czech SA accepted in accordance with Article 56 of the GDPR the role of a lead supervisory authority and investigated the complaint.

The Czech SA in its letter of 23 November 2021 requested the Company in accordance with Article 31 of the Regulation (EU) 2016/679 to cooperate and asked for the following information and supporting documents: what was the outcome of the investigation of the incident relating to _____ case, specifically in the part dealing with when it was sent to his e-mail address the order confirmation containing another person´s personal data, and why the complainant´s message of 28 February 2021 was not appropriately replied at first, and how the internal procedure is regulated as to the handling of data subjects´ requests made to apply their rights pursuant to the Regulation (EU) 2016/679 including the Company´s internal provisions (if any) regulating these procedures.

Úrad na ochranu osobných údajov | Hraničná 12 | 820 07 Bratislava 27 | Slovenská republika
tel.: 02/32313214 | fax: 02/32313214 | e-mail: statny.dozor@pdp.gov.sk | www.dataprotection.gov.sk

In reply to the said request received the Czech SA on December 3, 2021 the Company's statement in which it documented:

- Internal investigation of 24 March 2021, conclusions from this internal investigation that the Company conducted after it received the complainant's notice of 9 March 2021.
- Account statement by which the Company has proven that the order in question was picked up and paid.
- Chart describing the process of handling of requests including exercise of the data subjects' rights which shows that unless a customer request relates to blocking or erasure of personal data, it shall be passed by the operator on to the Company's DPO for further processing.
- Controller's Guidelines – Customer Requests to Block, Rectify, or Erase Personal Data No: 2019-08-05, which describes how the customer line operator shall act on a customer request as to the blocking or erasure of personal data.
- Controller's Guidelines – Non-Standard Customer Requests and Exercise of Rights Pursuant to the GDPR No: 2019-08-08. This document shall be used "if a customer of a legal representative requests, in relation to the GDPR, to exercise any of its rights (excluding blocking of commercial channels and/or erasure of personal data that is dealt with in the guidelines 2019-08-05) or if they request information on personal data that it not possessed or have not to be at the supplier's disposal, it is qualified as "non-standard request", similarly as in the case when the supplier would be informed (by whoever) about a potential security threat for NaturaMed (e.g. leak of confidential information, personal data, or of other data)". This document does oblige the customer line operators to pass the above specified customer requirements without delay on to the person nominated by the Company, i.e. to the Company's data protection officer (DPO) and to the Procedural department – customer care in copy.
- The order form – record from the internal system by which the Company has proven that the e-mail address was entered into the order form. Consequently, the Company used for sending of the order confirmation the e-mail address provided by the order party.

Concerning the complaint, the Company also stated that the internal investigation has not confirmed the information declared by the customer, i.e. neither a bulk leak of data, nor a leak which could have substantially influenced risks for data subjects. The conducted internal investigation revealed that no security incident occurred, neither was it confirmed that the order was placed by a third party. Form the NaturaMed's view, it was a standard order placed by the customer whereas, based on the mutually confirmed conditions and of the closed purchase contract, the goods were dispatched and paid for by the order party in a standard manner. So that the commitments and claims were mutually settled, and the closed deal seemed to be free of problems until the reception of the customer's e-mail communication. Neither the internal investigation has confirmed the possibility of entering the data by a third party. In such cases any payment for goods normally occurs, not even by the customer himself". The Company also points out that the complainant contacted it as late as 20 days after the reception of the e-mail message confirming the order and after the order had been picked up and paid. This was evidenced by the Company by a copy of the given order form,

Úrad na ochranu osobných údajov | Hraničná 12 | 820 07 Bratislava 27 | Slovenská republika
tel.: 02/32313214 | fax: 02/32313214 | e-mail: statny.dozor@pdp.gov.sk | www.dataprotection.gov.sk

the bank account statement, the copy of the communication exchange with the complainant, and by the copy of the internal investigation performed.

As to the other part of the complaint, the Company stated that *"The employee at the customer centre, instead of forwarding the non-standard communication to NaturaMed, she has blocked the commercial channels as well as the customer card of the complainant, which would in any case be carried out in the very next step, but she firstly misunderstood the substance of the customer request whereby she did not meet the requirements provided in the guidelines on non-standard requests, where it is clearly said that: "In case of any non-standard customer request, the staff member redirects without delay the communication towards NaturaMed onto the dedicated contact points. She did this only after the next reaction of the customer". Consequently, the information was forwarded belatedly which could have affected the potentially notified event. The matter was rectified in relation to the subsequent communication with the employee in that the given instruction was met and the case forwarded to NaturaMed on the next day. This situation has not any substantial impact on the conclusions from the internal investigation. NaturaMed apologized to the customer for an incorrect assessment of the importance of his notice (misunderstanding) on the customer centre side".* The above mentioned company has provided as evidence a chart describing the process of requests handling including exercise of the data subjects' rights; Controller's Guidelines – Customer Requests to Block, Rectify, or Erase Personal Data No: 2019-08-05; Controller's Guidelines – Non-Standard Customer Requests and Exercise of Rights Pursuant to the GDPR No: 2019-08-08.

The Czech SA assessed the Company's conduct related to the sending of order confirmation to the complainant's e-mail address. The Company has sufficiently proven by the internal investigation and by the copy of the order form that the e-mail address of the complainant was entered by the order party to the order form. The Company used for the dispatch of the order confirmation the e-mail address filled in by the order party so that no data security breach occurred on the controller's side and the Company did not have any obligation to notify the Office of a data breach pursuant to Article 33(1) of the GDPR.

Based on the above mention findings the Czech SA states that the Company proceeded correctly, when based on the complainant's notice pointing to a suspicion that inaccurate data were processed, it blocked these data in its database. The Company also, upon the complainant's notice, checked the incident and informed the complainant about the outcome of the investigation. Thus, the Company complied with the obligations of a controller defined in the GDPR.

In view of the above, the Czech supervisory authority proposed to reject a complaint in accordance with Art. 60 par. 8 GDPR.

The Office hereby in accordance with Art. 60 (8) of the GDPR accepted the decision of the Czech supervisory authority to reject the complaint against the company NaturaMed Prahraceuticals s.r.o. and consider the matter as closed in view of the findings of the Czech supervisory authority as the leading supervisory authority for cross-border processing of personal data.

Úrad na ochranu osobných údajov | Hraničná 12 | 820 07 Bratislava 27 | Slovenská republika
tel.: 02/32313214 | fax: 02/32313214 | e-mail: statny.dozor@pdp.gov.sk | www.dataprotection.gov.sk

On the basis of abovementioned findings, the Slovak SA decided to discontinue the proceeding regarding the complaint pursuant to Sec. 100 (5) (a) of the Slovak Data Protection Act.

Should the new relevant facts be identified, the case could be reviewed in the personal data protection proceedings.

Head of the Department
of administrative proceedings
Office for Personal Data
Protection of the Slovak Republic

Úrad na ochranu osobných údajov | Hraničná 12 | 820 07 Bratislava 27 | Slovenská republika
tel.: 02/32313214 | fax: 02/32313214 | e-mail: statny.dozor@pdp.gov.sk | www.dataprotection.gov.sk