STATE DATA PROTECTION INSPECTORATE

DECISION
REGARDING THE COMPLAINT OF [redacted] OF 25 JUNE 2022

5 August 2025 No. 3R-1007 (2.13-1.E)
Vilnius

State Data Protection Inspectorate (hereinafter the Inspectorate) on 2 September 2022 received the complaint of the applicant [redacted] (hereinafter the Applicant) dated 25 June 2022 concerning the actions of the company Vinted, UAB (hereinafter the Company), which was forwarded by the Spanish supervisory authority via the Internal Market Information system (IMI) (Inspection reg. No 1R-5026 (2.13.Mr)) (hereinafter referred to as the Complaint).

In the Complaint, the Applicant stated that on 2 April 2022 he was informed by the Company about the blocking of his account. According to the Applicant, the Company falsely claimed that the Applicant used multiple accounts and linked him to illegal activity related to the sale of counterfeit goods carried out through other accounts. The Applicant notes that on 16 May 2022 he contacted the Company with requests to access the data and to rectify them, but these requests were not answered. Instead, the Applicant received from the Company a notification refusing to take action regarding the right to be forgotten.

The Inspectorate, competent to act as the lead supervisory authority and to adopt final decision regarding the Applicant's Complaint (Article 56 of 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, repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter GDPR), Article 56, Article 60(7)),

established:

The Inspectorate received the Company's reply dated 2023-02-02 (Inspectorate reg. No. 1R-912 (2.13.Mr)) (hereinafter the Response), in which the Company explained that the Applicant's account was blocked for violating the platform rules and deleted on 2022-07-02 in accordance with the standard personal data retention periods. Accordingly, at the time of submitting the Response, the Company processed a very limited amount of the Applicant's personal data, due to which the Company cannot specify to the Inspectorate exactly which of the Applicant's personal data were processed before the account deletion. The Company noted that it undoubtedly processed data which every registering user must provide (password, e-mail address), as well as other data depending on which specific functions the Applicant used, for example, whether he had posted advertisements and traded on the platform, or only bought goods, whether he had left or received feedback, whether he had uploaded a free-form profile description, and so forth.

In response to the Inspectorate's questions related to the possession of multiple platform accounts and the proper implementation of the accuracy principle, the Company indicated that considering the

limited data available about the Applicant at the time of the Response submission, the Company is unable to provide detailed explanations and evidence regarding the proper implementation of the accuracy principle. According to the Company, upon establishing that the Applicant violated the requirements of Vinted's General Terms by creating more than one account, his account was blocked and, as seen from the submitted correspondence, when the Applicant contacted the customer service department, the Applicant's situation was re-evaluated and it was confirmed that the Applicant's account was blocked justifiedly. Accordingly, the Company considered that it properly implemented the data accuracy principle.

Regarding the Applicant's right to access data and to request correction, the Company stated that it received these requests on 16 May 2022 and provided the respective response on 17 May 2022, however, the customer service specialist improperly assessed the nature of the Applicant's request, therefore replied to the Applicant not regarding the right to access and rectify data, but regarding the inability to delete the account, i.e. concerning the implementation of the right to erasure. On 17 May 2022, the Applicant submitted a repeated request through the customer service system regarding the exercise of data subject rights, which was not answered in a timely manner due to human error. The Applicant's request was answered upon detection of this error, i.e. on 1 February 2023.

Taking into account the circumstances indicated in the Complaint and the Response, the Inspectorate considers that the fundamental dispute between the parties relates to the potentially improper exercise of the Applicant's rights as a data subject (the right of access to data and the right to request correction (GDPR Articles 12, 15, 16)) and the potentially improper implementation of the data accuracy principle (GDPR Article 5(1)(d)).

Regarding the exercise of the Applicant's right of access to data and the right to request rectification

During the examination of the complaint, it was established that on 2 April 2022 the Applicant's platform account was blocked due to violation of the platform rules – the Company determined that the Applicant had created multiple accounts, which contradicts the prohibition set out in Article 11.2 of the platform's General Terms. On the same day, the Applicant contacted the Company's customer service specialists requesting to "correct the error". The Company, in turn, indicated that the Applicant's case was reviewed again, but the initial decision would remain unchanged and "the account will remain blocked".

On 16 May 2022, the Applicant applied to the Company with a request for access to the data (Article 15 of the GDPR), noting that he considers the data held (processed) by the Company to be inaccurate. Regarding the inaccuracy of the data, the Applicant indicated that the Company incorrectly linked the personal data of his account with the data of another account and accordingly unreasonably applied the blocking of the account on this basis (Article 16 of the GDPR).

On 17 May 2022, the Company submitted a response stating that "*We have examined your request. Your request does not meet the requirements for the application of the right to erasure set out in Article 17 of the EU General Data Protection Regulation (GDPR).*" <...>". On the same day, the Applicant again contacted the Company indicating that he was not requesting the right to delete data, but the exercise of rights of access and rectification.

The Inspectorate notes that the Company replied to the Applicant's repeated request for access to data only on 1 February 2023, i.e. only after the Inspectorate contacted the Company with an instruction to demonstrate the compliance of its actions with the GDPR provisions. The Company did not respond at all to the Applicant's request to rectify data. The Inspectorate also emphasises that both when responding to the Inspectorate and when belatedly responding to the Applicant's request for access to data, the Company had already deleted the majority of the Applicant's personal data.

Article 15 of the GDPR regulates the data subject's right of access to data. Article 15(1) of the GDPR provides that the data subject has the right to obtain from the data controller confirmation as to whether or not personal data concerning them are being processed, and, where such personal data are processed, the right to access the personal data and the information referred to in points (a) to (h) of that paragraph. Articles 15(3) and (4) of the GDPR establish that the data controller shall provide a copy of the personal data undergoing processing requested by the data subject, but the right to obtain a copy shall not adversely affect the rights and freedoms of others.

Article 16 of the GDPR provides that the data subject has the right to require the data controller to rectify inaccurate personal data concerning them without undue delay. Taking into account the purposes for which the data were processed, the data subject has the right to require incomplete personal data to be completed, including by means of providing a supplementary statement.

Article 12(2) of the GDPR provides that the data controller shall facilitate the exercise of the data subject's rights set out in Articles 15 to 22. Paragraph 3 of the same Article provides that the data controller shall communicate the information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. Where the data controller does not take action on the data subject's request, the data controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Article 12(4) GDPR).

In European Data Protection Board Guidelines No. 01/2022 on the right of access to data, it is stated that the overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they are informed and can verify the lawfulness of such processing and the accuracy of the data processed. This right is a means by which favourable conditions are created for an individual to exercise other rights, such as the right to request erasure or rectification of data.

In the case under consideration, it is evident from the circumstances established during the examination of the Complaint that the Applicant's right of access to data, enshrined in Article 15 of the GDPR, as well as the right to request rectification of data, enshrined in Article 16 of the GDPR, were not fulfilled and, accordingly, were violated.

Although on 16 May 2022 the Applicant contacted the Company clearly indicating disagreement with the applied account blocking and seeking to access the processed data and request their rectification, the Company replied to the Applicant stating that it would not take action on the alleged request concerning the right to erasure. This means that the Company not only failed to take action on the Applicant's requests but also generally did not properly establish the nature and substance of the Applicant's requests.

On 17 May 2022, when the Applicant again contacted the Company clearly indicating that he wished to exercise the right of access to data and the right to request their rectification, this request by the Applicant was not answered at all, i.e., the request was essentially ignored.

Accordingly, the Inspectorate assesses that by improperly determining the nature of the Applicant's request of 16 May 2022 and by not responding at all to the Applicant's repeated request of 17 May 2022, the Company violated the provisions of Articles 12(3), 15(1) and (3), and 16 of the GDPR.

The above assessment by the Inspectorate is not altered by the circumstance that on 1 February 2023 the Company eventually provided a response to the Applicant's request for access to data. Such a conclusion is drawn for the following reasons:

Firstly, the response to the Applicant was provided only after receiving the Inspectorate's instruction of 20 January 2023 to provide information in implementing the accountability principle[1], i.e.,

[1] Inspectorate registration No. 2R-371 (2.13.Mr).

the response to the Applicant was given only upon being informed that the supervisory authority had initiated an investigation against the Company for failure to respond.

Secondly, at the time the response was provided, the Company had already deleted the majority of the Applicant's personal data[2], which were relevant to the Applicant's intention to effectively and realistically exercise the right to request rectification. This means that due to the data deletion and the delayed provision of the response[3], the actual exercise of the Applicant's right of access to data became essentially impossible and meaningless.

Finally, by not receiving the necessary information in a timely manner, the Applicant was also prevented from effectively exercising the right to request rectification of data and accordingly proving the unjustification of the account blocking.

On the basis of the above circumstances and legal norms, the Applicant's Complaint regarding the improper implementation of the data subject's rights to access data and to request rectification is recognised as justified.

Regarding the proper implementation of the data accuracy principle

In the Complaint, the Applicant indicates that the Company incorrectly linked his personal data with another person's data, thus violating the principle of accuracy.

Article 5(1)(d) of the GDPR provides that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (principle of accuracy).

Article 29(1)(4) of the Republic of Lithuania's Law on Legal Protection of Personal Data (hereinafter LLPPD) provides that the supervisory authority shall adopt a decision to terminate the examination of a complaint or part thereof if, during the examination of the complaint or part thereof, it becomes apparent that the complaint or part thereof cannot be examined due to lack of information or other significant circumstances.

The Inspectorate notes that the decision it adopts after examining the complaint shall be considered an administrative decision[4], and therefore must comply with the criteria of legality and reasonableness set out in Article 10(5) of the Republic of Lithuania Law on Public Administration (hereinafter the LAP). Pursuant to Article 10(5)(5) of the LAP, an administrative decision must, among other things, specify the legal and factual basis of the administrative decision or other circumstances affecting the administrative decision. It should be noted that this requirement is inherently linked to the principle of objectivity enshrined in Article 3(9) of the LAP, which means that the adoption of an administrative decision and other official acts of a public administration body must be impartial and objective. The Lithuanian Supreme Administrative Court (hereinafter the LSAC) has stated that in compliance with the principle of objectivity, decisions of public administration bodies must correspond to the true factual circumstances, which are established by clarifying all circumstances relevant to the decision-making and by critically and impartially assessing the evidence [5]. This means that individual

[2] In its response to the Inspectorate, the Company stated that the majority of the Applicant's personal data were deleted on 2 July 2022 in accordance with the standard personal data retention periods.

[3] Article 12(3) of the GDPR establishes a general rule that responses to data subject requests must be provided without undue delay, but in any event no later than one month after receipt. In the context of the Complaint under consideration, the response to the Applicant's request of 16 May 2022 should have been provided by no later than 16 June 2022.

[4] An administrative decision is a one-off will of a public administration body expressed in a manner and/or form regulated by legal acts, mandatory and intended for a specific person or an individually defined group of persons (Article 2(5) of the LAP).

[5] For example, the decision of LSAC of 14 April 2014 in administrative case No. A662-1010/2014.

administrative decisions cannot be based on guesses or suspicions, personal sympathies or antipathies[6], but must be substantiated in such a way that there is no doubt regarding the outcome of the decision[7].

In the case under review, it was established that on 2 July 2022 the Company deleted the majority of the Applicant's personal data, including those from which it would be possible to objectively determine whether the Company properly implemented the principle of data accuracy arising from Article 5(1)(d) of the GDPR. Due to this circumstance, the Inspectorate is unable to determine whether the Company properly implemented the principle of data accuracy. The supervisory authority concerned to which the Complaint was submitted (in this case, the Spanish supervisory authority) adopts the final decision regarding the part of the Complaint to be dismissed and informs the Applicant thereof, as well as notifying the Company (Articles 60(8) and (9) of the GDPR).

Notwithstanding the above, the Inspectorate notes that the lack of information preventing the determination of all circumstances necessary for a proper examination of the Complaint was caused by the Company's actions in deleting the necessary information on 2 July 2022. Accordingly, the Inspectorate will further address in this decision the implementation of the accountability principle established in Article 5(2) of the GDPR in the context of the Complaint.

Regarding the implementation of the accountability principle

As already noted, in absence of objective data regarding the data processed by the Company at the time of the Applicant's requests, the Inspectorate is unable to assess the compliance of such data processing with the GDPR provisions. Nevertheless, the Inspectorate considers that this circumstance must be assessed in the context of Article 5(2) of the GDPR. Otherwise, data controllers could always avoid violations of GDPR compliance simply by deleting data relevant to such investigations.

Article 5(2) of the GDPR provides that the data controller is responsible for, and must be able to demonstrate compliance with, paragraph 1 (the accountability principle).

Article 24(1) of the GDPR provides that, taking into account the nature, scope, context, and purposes of data processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons, the data controller implements appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is carried out in compliance with this Regulation. These measures are reviewed and updated as necessary.

The LSAC has stated in its practice that the essence of the accountability principle is that the data controller must: to establish measures which under normal circumstances would help ensure compliance with data protection rules during data processing operations, and have available documentation from which data subjects and supervisory authorities can see the measures taken to ensure compliance with data protection rules.[8]

In the case under review, it was established that the deletion of the Applicant's personal data (and relevant evidence that the data accuracy principle arising from Article 5(1)(d) of the GDPR was properly implemented) was caused by the expiry of the standard personal data retention period (3 months) set by the Company. Upon expiry of this period, the data were automatically deleted.

It should be noted that the GDPR does not set specific personal data retention periods. Determining appropriate data retention periods that comply with the principle of data minimisation is the obligation of the data controller[9]. According to the Inspectorate's assessment, data retention periods must

[6] LSAC ruling of 17 November 2014 in administrative case No. A858-2430/2014.
[7] LSAC ruling of 8 September 2015 in administrative case No. A-2494-438/2015.
[8] LSAC decision of 29 December 2021 in administrative case No. eA-2483-822/2021.
[9] Recital 39 of the GDPR provides that personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed; to that end, it is first of all necessary to ensure that the storage period for personal data is truly minimal.

be established taking into account all circumstances related to the specific processing. This means that the data controller must not only ensure the timely deletion of unnecessary data but also ensure that certain data are retained longer (deviating from standard data deletion periods), considering the possible need to prove compliance of the performed data processing with GDPR provisions.

As seen from clause 2.8.4[10], of the Company's privacy policy relevant to the Complaint, the Company provides for the retention of personal data for a longer period, taking into account the need to defend its rights and interests in the event of a dispute. In the context of this privacy policy provision, it is also relevant to consider the Company's explanations to the Inspectorate dated 17 February 2022 (Inspectorate's reg. No.1R-968 (2.13.Mr)), in which the Company clarified that it interprets the concept of "dispute" as a situation where personal data are retained for the purpose of defending against potential claims or conflicts, when it becomes evident that a certain fact or legal issue is perceived differently by the user than by the Company, and due to such disagreement the Company may need to protect its rights and legitimate interests. Such disputes include cases where the user files a complaint with the consumer protection authority or the personal data protection supervisory authority.[11]

In the present case, as is evident from the communication between the parties, the Applicant categorically disagreed with the basis for blocking his account and accordingly contested it. Moreover, in correspondence with the platform's customer service specialists, the Applicant explicitly stated that if he did not receive the requested information from the Company, he would "contact the Data Protection Agency".[12] Given that the Applicant's dispute regarding the possible inaccuracy of his personal data and the corresponding account blocking was not resolved by the customer service specialists[13], nor was he provided with the requested data, and given that the Applicant expressed a direct intention to contact the supervisory authority, the Inspectorate considers that the Company had clear indications that the Applicant's personal data (to the extent necessary to demonstrate compliance with the requirements of Article 5(1)(d) of the GDPR) needed to be retained further in order to implement the accountability principle arising from Article 5(2) of the GDPR.

Based on the circumstances indicated, the Inspectorate concludes that, in the context of the examined Complaint, being unable to justify proper implementation of Article 5(1)(d) of the GDPR, the Company violated the accountability principle of the data controller as set out in Article 5(2) of the GDPR.

Regarding the imposition of corrective measures on the Company

Article 31(2)(1) of the LLPPD provides that when a complaint or part thereof is found justified, the Inspectorate issues instructions, recommendations and/or applies other measures prescribed by laws regulating personal data and/or privacy protection to the data controller and/or data processor. Pursuant to Article 12(2)(5) of the LLPPD, the Inspectorate has the right to provide data controllers, data processors and other legal or natural persons with recommendations and instructions concerning personal data processing and/or privacy protection.

[10] Clause 2.8.4 of the privacy policy provides that if you engage in a dispute with Vinted or if it is necessary to enforce its Rules or otherwise defend, ensure enforcement, exercise or maintain its rights, we will collect and use all personal data held by Vinted to find a resolution to the specific situation. Such collection and use is based on the legitimate interest of protecting Vinted's rights and interests (Article 6(1)(f) of the GDPR). For this purpose, the collected and used personal data are retained for 5 (five) years from the moment we determine the need to defend our specific rights and interests, and in the case of a dispute – until the final compulsory execution of the decision of the authorised authority.

[11] Company's explanations to the Inspectorate dated 17 February 2022, p. 18.

[12] Company's Response Annex No. 3, p. 13.

[13] The Company's customer service specialist, communicating with the Applicant and responding to the latter's intention to contact the supervisory authority, stated that "I regret that you do not like our working procedure, but if you wish to continue by submitting a complaint, we can only wish you good luck."

Recital 129 of the GDPR provides that any measure applied by a supervisory authority must be appropriate, necessary, and proportionate to ensure compliance with this Regulation, taking into account the circumstances of each individual case. It should be noted that the LLPPD provides the Inspectorate with discretionary power, upon recognising a complaint as justified, to select corrective measures, provided that each measure applied by the Inspectorate is appropriate, necessary, and proportionate, taking into account the infringement.

Article 58(2)(b) of the GDPR provides that each supervisory authority is empowered to issue reprimands to the data controller or data processor where processing operations have infringed the provisions of this Regulation.

Taking into account that the Inspectorate has no information indicating that the infringements established by this decision are of a systemic nature (i.e. affecting not only the Applicant but also other users of the platform), a reprimand is issued to the Company for infringements of Article 12(3), Article 15, Article 16, and Article 5(2) of the GDPR.

In the view of the Inspectorate, the issuance of additional corrective measures (instructions) related to the exercise of the Applicant's rights would be inappropriate, given that the personal data the Applicant sought to access and rectify have already been deleted, making the proper exercise of his rights (the right of access and the right to rectification) objectively no longer possible.

In accordance with the above, as well as Article 31(1)(1), Article 31(2)(1) of the LLPPD, Article 58(2)(b), Article 60(7) of the GDPR, the Inspectorate

hereby decides:

1. To recognise the Applicant’s Complaint in the part concerning improperly implemented rights to access data and to request rectification as justified.

The supervisory authority concerned to which the Complaint was submitted (in this case, the Spanish supervisory authority) adopts the final decision regarding the part of the Complaint to be dismissed and informs the Applicant thereof, as well as notifying the Company (Articles 60(8) and (9) of the GDPR).

2. To determine that being unable to justify proper implementation of the data accuracy principle in the context of the Applicant’s Complaint, the Company violated the accountability principle established in Article 5(2) of the GDPR.

3. To issue a reprimand to the Company.

4. To inform the Company and the Applicant of the decision adopted.

This decision may be appealed to the Regional Administrative Court within one month from the date of its delivery in accordance with the procedure established by the Law on Administrative Proceedings of the Republic of Lithuania (address: Žygimantų g. 2, Vilnius).

Director [redacted]