STATE DATA PROTECTION INSPECTORATE

DECISION
ON THE COMPLAINT OF [redacted]

May 2025 No. 3R-516 (2.13-1.E)
Vilnius

On 3 February 2020, the State Data Protection Inspectorate (hereinafter referred to as 'the Inspectorate') received a Complaint from the Complainant [redacted] (hereinafter referred to as 'the Complainant') forwarded by the French data protection supervisory authority (Inspectorate Reg. No 1R-797 (2.13)) (hereinafter referred to as 'the Complaint'). The Complainant states in the Complaint that Vinted, UAB (hereinafter referred to as 'the Company') on 20/07/2019 sent an email stating that access to Complainant's account was blocked for security reasons. The Complainant was asked to send several supporting documents to prove her identity. The Complainant replied, that she did not want to send these documents to the Company and asked to delete her account if it was not possible to unblock it. The Complainant stated that she had received a response from the Company, assuring that it had the right to request this information under 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 referred to as the GDPR) and the Complainant responded to this letter stating that she wanted the account to be deleted and could not do so herself as the access to the account was blocked. The Complainant was informed that her conversation with the Company is closed until the requested documents are provided to the Company.

Together with the Complaint the Inspectorate was provided with communication documents between the Company and the Complainant. According to communication between the parties, on 21/07/2019 the Company replied to the Complainant by indicating that her account is blocked due to suspicious activity and that the account might be used by an unauthorized third party. By this same email the Complainant was asked to provide: 1) a photo of the credit card used for most recent purchases, showing only the identity of the card owner, the last 4 digits and the expiry date; or 2) a screenshot of the bank statement showing the last bank withdrawal made by the Company; or 3) a utility bill or another bill with the Complainant's address clearly visible (except mobile phone bill). The Company indicated that such additional information from the Complainant is required to "*help authenticate her account*".

The Complainant in turn replied that she recently submitted her telephone number to the Company in order to log in to her account and that she refuses to provide any more additional information. Complainant also noted that her account was linked to her Gmail account (through which she contacted the Company) as well as that she has made multiple purchases through the platform and thus the Company already had enough information to identify her. The Complainant indicated that in the event the unblocking of her account would still be impossible without the requested documents, she would like her account and all associated personal data deleted.

On 07/24/2019 the Company replied to the Complainant that "*to ensure data security on our platform and in accordance with Article 32, Art. 5 (1) (f) and Article 12 of the General Data Protection Regulation, Vinted has the right to information to identify members*."

The Complainant in turn provided that she does not wish to provide the requested documentation and once again requested her data to be deleted.

The Company then provided that "*it is impossible to delete the account when it is blocked*" and before the Complainant's account is unblocked, the Company needs to make sure it is contact with the owner of the account. Right after this the Company indicated once more that before

unblocking the account it is need to be sure that the account is secure and that if the Complainant does not provide requested documents the Company will not be able to answer further inquiries regarding blocking and will close the conversation with the Complainant.

The Inspectorate, being in the position to act as the lead supervisory authority in accordance with Article 56 GDPR and prepare a final decision under Article 60(7) GDPR,

has established that,

The Inspectorate received the Company's 3 April 2020 response (Inspectorate Reg. No 1R-2378(2.13.E)) (hereinafter referred to as 'the Response'), in which the Company confirmed, that it processes the Complainant's personal data and pointed out that the Complainant's account was blocked due to suspicions that a third party may have gained unauthorized access to the Complainant's account. The Complainant requested to delete her personal data by contacting the Company's customer service via the dedicated electronic system. The Complainant was given answers via internal notification system. The Company stressed, that since the Complainant did not agree to confirm her identity, and the Complainant's account, as mentioned, was blocked due to suspicions that third parties may have gained unauthorized access to her account, the Company could not implement the Complainant's right to be forgotten due to the fact that it cannot determine the identity of the person who submitted the request (Article 12(2) of GDPR).

The Inspectorate, having established the above-mentioned circumstances further in this decision provides an assessment on the Complaint.

Article 12(2) of GDPR provides that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Article 12(1) of the GDPR mandates that any communication regarding data subject rights must be concise, transparent, intelligible, and easily accessible, using clear and plain language. In accordance with Article 12(4) of the GDPR, the controller is obliged to provide the following information: (a) the reasons for not taking action, (b) information on the possibility of lodging a complaint with a supervisory authority, and (c) information on the possibility of seeking a judicial remedy. Given that the transparency requirements apply throughout the processing cycle, the controller must ensure the quality and completeness of the information provided for each element specified in Article 12(4) of the GDPR.

Having assessed the communication between the parties, it is evident that the Company's response and actions taken fail to meet the requirements set out in Articles 12(1) and 12(4) of the GDPR.

As established above, on 21/07/2019 and 24/07/2019, the Complainant submitted requests under Article 17 of the GDPR for the deletion of her account. Instead of assessing the situation in accordance with Article 17 and providing quality information in line with Article 12(4), the Company merely stated that it is "*impossible to delete a blocked account*" and proceeded to request further identity documentation to "*unblock*" the account. The Company also informed the Complainant that if the requested documentation was not provided, the conversation regarding the unblocking of the account would be closed, and the Complainant would not be able to submit further requests.

This response indicates that the Company refused to unblock the Complainant's account and claimed that it could not identify her for this purpose. However, the Company failed to clearly and transparently explain to the Complainant that it could not fulfill her request in accordance with Articles 11(2), 12(2), and 12(6) of the GDPR. Simply stating that it is "*impossible to delete a blocked account*" does not satisfy the Company's obligation to provide the Complainant with clear and understandable reasons for its inaction, as required under Article 12(1) of the GDPR.

Furthermore, according to Article 12(2) of GDPR the controller not only has the right to request additional information regarding the data subject's identity, but also has an obligation to demonstrate that it is not in a position to identify the data subject.

Given this, the Inspectorate also points out that the Complainant encountered further confusion in exercising her right to be forgotten due to additional factors. Specifically, after the Complainant successfully passed two-factor authentication using her phone number[1] and communicated with the Company via the email address linked to her account, the Company not only requested further identification but also failed to explain why the use of her phone number and email was insufficient to exercise her rights under Article 17 of the GDPR. This lack of clarification led to further confusion for the Complainant, thus leading to violation of Article 12(1) of the GDPR.

Additionally, the Inspectorate notes that after refusing to take action in accordance with Article 17 of the GDPR, the Company failed to provide the Complainant with (1) information on the possibility of lodging a complaint with a supervisory authority and (2) information on the possibility of seeking a judicial remedy. This further confirms the breach of Article 12(1) of the GDPR and also demonstrates non-compliance with the requirements of Article 12(4).

In conclusion, Inspectorate concludes that the Company's response failed to meet the requirements set out in Articles 12(1) and 12(4) of the GDPR.

It should be noted that the Inspectorate, in cooperation with the French data protection supervisory authority, has received information from the Applicant on 05/09/2024 that the Applicant is interested in the further examination of the Complaint. In view of the above, the Inspectorate considers that the Applicant continues to seek to exercise the right to be forgotten under the GDPR and is therefore interested in receiving transparent and clear information on the exercise of this right.

Based on the aforementioned circumstances and in accordance with Article 31(2)(1) of the Law on Legal Protection of Personal Data (hereinafter referred as "LLPPD") and Article 58(2)(d) of the GDPR, the Inspectorate orders the Company to provide the Complainant with reasons in a fair and transparent manner on why no action was taken in regards to her request pursuant to Article 17 of the GDPR.

The Inspectorate notes that this decision has been coordinated with the supervisory authorities concerned (France, Poland, Spain, the Netherlands and Germany) on 16/04/2025 in accordance with Article 60(6) of the GDPR.

In accordance with Article 31(1)(1), 31(2)(1) of the LLPPD, Article 60(7) GDPR, the Inspectorate

hereby decides as follows:

1. To declare that upon receipt of the Complainant's request to erase her personal data, the Company did not in a clear and transparent manner provide the Complainant with reasons for its inaction in accordance with Article 12(1) and did not provide all the required information in accordance with Article 12(4).

2. To order the Company:

2.1. To provide the Complainant with clear and transparent reasoning as to why no action was taken in response to her request for erasure under Article 17 of the GDPR within 1 (one) month of receipt of this decision;

Deputy Director,
acting as Director [redacted]

[1] In the Response the Company indicated that "on 20/07/2019 the Complainant, after providing her telephone number, received SMS code, which she immediately (08:47) used to confirm her identity".