STATE DATA PROTECTION INSPECTORATE

DECISION
REGARDING THE COMPLAINT OF [redacted] OF 19 FEBRUARY 2021

5 August 2025 No. 3R-1005 (2.13-1.E)
Vilnius

State Data Protection Inspectorate (hereinafter the Inspectorate) on 2021-05-03 received the complaint of the applicant [redacted] (hereinafter the Applicant) dated 2021-02-19 concerning the actions of the company Vinted, UAB (hereinafter the Company), which was forwarded by the German supervisory authority via the Internal Market Information system (IMI) (Inspectorate reg. No 1R-3125 (2.13.Mr)) (hereinafter referred to as the Complaint).

In the Complaint, the Applicant stated that one day she unexpectedly could no longer access her account on the Company's platform, as she was required to provide her mobile phone number and thus verify her account. The Applicant also stated that she could not access the account in order to edit or delete it. According to the Applicant, she had not been properly informed about the processing of her phone number. The Applicant stated that she was informed she could not use the Company's platform without providing her mobile phone number.

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

established:

The Inspectorate received the Company's reply dated 2021-06-25 (Inspectorate reg. No. 1R-4502(2.13.)) (hereinafter the Reply), in which the Company indicated that the Applicant had been asked to provide her mobile telephone number for the purpose of mandatory phone number verification, which is carried out to prevent fraud and to ensure the security of the company's platform and its members. A mobile number is requested for security purposes when suspicious login activity is detected, for example, when a user logs in from another country. The Company explained that when the Applicant attempted to log in, a standard phone number verification window was displayed to her. The Company stated that the legal basis for such personal data processing was the performance of the contract with the Applicant (sub-clause 1.5 of the platform's general terms and conditions (hereinafter the Rules)), in accordance with the lawful basis for personal data processing set out in Article 6(1)(b) of the GDPR.

In the reply to the Inspectorate dated 2023-07-28 (Inspectorate reg. No 1R-5341 (2.13.Mr)) (hereinafter the 2023-07-28 Reply), the Company stated that the Rules constitute a legally binding agreement between the user and the company regarding access to and use of the Company's platform. Ensuring the security of the platform of the Company and the related application of security procedures and restrictions on the use of the platform are an integral part of the contract and one of the essential

elements of the contract. Phone number verification is one of the procedures for ensuring account security. Both the Company's right to apply such a procedure to the consumer and the restrictions that the consumer faces until the telephone number is confirmed arise directly from the Rules as a contract. According to the Company, as the operator of an e-commerce platform, it has a legitimate expectation to implement measures that ensure the security of the platform and prevent unlawful actions. It should be considered that platform users have an expectation that the Company will make reasonable efforts to ensure that the platform and user accounts created on it are protected from malicious third-party activity. It may also be considered that an average user who has created an account on an e-commerce platform may expect that, for the safety of both themselves and other users, certain proportionate security measures may be applied. Therefore, according to the Company, the processing of data whereby the user is requested to provide a phone number for verification when suspicious activity is detected in the account does not fall outside the scope of the Rules as a contract and is necessary for the performance of this contract. In the 2023-07-28 Reply, the Company also noted that mandatory phone number verification may only be waived in exceptional cases, when the individual contacts the Company explaining specific circumstances related to their situation. According to the Company, the principle of freedom of contract allows the parties to derogate from the existing contractual terms by mutual agreement; however, such derogation does not in itself negate the necessity of processing the telephone number in the circumstances provided for in the contract (the Rules), such as when suspicious activity is detected.

In the reply dated 2023-02-02 (Inspectorate reg. No. 914 (2.13.Mr)) the Company explained that, at the time the Applicant's telephone number was collected, the version of the privacy policy of the platform dated 2020-11-26 was in effect, in which the Applicant was provided with the information required under Article 13 of the GDPR.

Regarding the lawfulness of collecting the Applicant's telephone number

During the examination of the Complaint, it was established that the Company offers a platform (website and mobile application) where individuals can buy and sell clothes and other goods, i.e. individuals are given the opportunity to act as buyers and/or sellers of goods on the Company's platform. Once an individual becomes a member of the platform operated by the Company, i.e. upon completing the registration process, a contractual relationship is formed between the Company and the registered person. In this case, the Applicant had an account on the Company's platform, and consequently, a contractual relationship existed between the Company and the Applicant related to the implementation of the respective obligations, rights and duties. According to the Company, it collected the Applicant's telephone number in order to carry out mandatory phone number verification for the purposes of fraud prevention and ensuring the security of the Company's platform and its members. According to the Company, such data processing was carried out based on Article 6(1)(b) of the GDPR. In the Reply to the Inspectorate dated 2022-02-17 (Inspectorate reg. No 1R-968 (2.13.Mr)) the Company also noted (on page 9) that the Rules are part of the contract between the company and its users. According to the Company, each registered user of the platform must confirm, at the time of registration, that they have read and understood the Rules. In the 2023-07-28 Reply, the Company additionally noted that ensuring the security of the platform it operates, along with the application of related security procedures and platform usage restrictions, is an integral part of the contract and one of its essential elements. Therefore, the processing of data whereby the user is requested to provide a telephone number for verification purposes upon detection of suspicious activity in the account does not fall outside the scope of the Rules as a contract and is necessary for the performance of this contract.

In accordance with the GDPR, personal data may only be processed in compliance with the *principles* relating to the processing of personal data set out in Article 5 of the GDPR, and such data processing must be based on at least one lawful basis for personal data processing as provided for in

Article 6 and/or Article 9 of the GDPR, depending on the category of personal data being processed. Pursuant to Article 6(1)(b) of the GDPR, data processing is lawful if (and to the extent that) it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The European Data Protection Board (hereinafter EDPB), in its Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects (hereinafter the Guidelines), states that the necessity of data processing is a required condition for applying either of the options in Article 6(1)(b). The concept of what is "necessary for the performance of a contract" is not simply an assessment of what is permitted by the terms of the contract or what is included in it. The notion of necessity in European Union law has an autonomous meaning and must reflect the objectives of data protection law. The assessment of what is "necessary" relates to a general fact-based evaluation of the data processing in light of the pursued purpose and whether it is less privacy-intrusive compared to other alternatives that could achieve the same purpose. If there are realistic, less privacy-intrusive alternatives, the data processing is not "necessary". Article 6(1)(b) of the GDPR will not apply to data processing that is useful but, objectively, not necessary for providing the service specified in the contract or for taking appropriate steps at the data subject's request prior to entering into a contract, even if such processing is necessary for other business purposes of the controller (Guidelines, points 23, 25).

The Guidelines emphasise that the provision "processing is necessary for the performance of a contract to which the data subject is party": <...> must be interpreted narrowly and does not apply where the processing of the data subject's data is not genuinely necessary for the performance of the contract, but the controller carries it out unilaterally nonetheless. The mere fact that the processing of certain data is foreseen in the contract also does not always mean that it is necessary for the performance of the contract. The assessment of the necessity of data processing is clearly linked to compliance with the purpose limitation principle. It is important to determine precisely the rationale for entering into the contract, i.e. its essence and main purpose, as this will be used to assess whether the processing of data is necessary for the performance of the contract (p. 28, 29 of the Guidelines).

Accordingly, in order to assess whether the Applicant's personal data (telephone number) was lawfully processed on the basis of Article 6(1)(b) of the GDPR, it is necessary to establish whether such data processing was *objectively necessary* for the performance of the contract with the Applicant.

As already mentioned, the Company offers a platform (a website and application) through which individuals can buy and sell clothes and other goods, i.e. individuals are given the opportunity to act as buyers and/or sellers of goods on the company's platform. In its 2023-07-28 Reply, the Company stated that, acting as the operator of an e-commerce platform, it has a legitimate expectation to implement measures ensuring the security of the platform and preventing unlawful activities. According to the Company, users of the platform have an expectation that the Company will make reasonable efforts to ensure that the platform and the user accounts created on it are protected from malicious actions by third parties. The Company bases this position on Clause 1.5 of the Rules, which states that, *"for security reasons, VINTED may ask the USER to verify their ACCOUNT. This may be done, for example, by verifying the USER'S Facebook or Google account, the USER'S telephone number, the USER'S credit or debit card, a PIN code-based method, or other methods that VINTED may apply at its discretion."*

Having assessed the material collected during the examination of the Complaint, the EDPB's methodological materials, as well as the explanations provided by the Company, the Inspectorate concludes that the processing of the Applicant's telephone number could not be based on Article 6(1)(b) of the GDPR. Such a conclusion is to be drawn on the basis of the following arguments.

First, the Company failed to demonstrate the objective necessity required by the essence and objectives of the regulation laid down in Article 6(1)(b) of the GDPR. The Company justifies the necessity of such data processing by stating that a "*typical user who has created an account on the e-*

commerce platform may expect that, to ensure the security of both their own and other users of the platform, certain proportionate security measures may be applied to them. Therefore, the data processing in which the user is requested to provide a telephone number for the purpose of confirmation following the detection of suspicious activity in the account does not go beyond the Rules as a contract and is necessary for the performance of this contract." Nevertheless, the Inspectorate assesses the Company's arguments as declarative and not substantiated by any objective reasoning or data.

As already stated, the assessment of what is "necessary" relates to a general, fact-based assessment of data processing in light of the pursued objective and whether it is less privacy-intrusive compared to other possible means of achieving the same goal[1]. Clause 1.5 of the Rules provides that *"In order to register, the USER must provide their user name (pseudonym),* ***email address*** *and password (directly or via a "Facebook" or "Google" account) so that the WEBSITE can identify the USER each time they log in."* As is evident from the Rules, the provision of a telephone number is only one of the means by which a particular person's account may be confirmed and, accordingly, the security declared by the Company ensured[2]. Considering that persons (including the Applicant), in order to register on the Company's platform, in all cases must provide their email address, and also that confirmation of this email address is one of the possible means of "account confirmation", the Inspectorate concludes that the provision of a telephone number is not objectively necessary for the performance of the contract (the Rules) concluded between the parties.

The circumstance that such data processing is not objectively necessary is further supported by the explanations provided by the Company during the examination of the Complaint. For instance, in the 2023-07-28 Reply, the Company indicated that *telephone number verification may be waived only in exceptional cases where a person contacts Vinted explaining specific circumstances related to their situation."* In its Guidelines, the EDPB has stated that the data controller should be able to demonstrate how the core subject matter of the specific contract with the data subject cannot in fact be fulfilled if the specific processing of personal data under consideration is not carried out.[3] Thus, the fact that the data subject has the possibility to contact the data controller (the Company) and request that the telephone number verification procedure not be applied further confirms that the contract with the data subject could have been performed without such data processing.

These conclusions of the Inspectorate are also confirmed by the data minimisation principle established in Article 5(1)(c) of the GDPR, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The importance of this principle in the context of online (digital) service contracts is also emphasised by the EDPB[4]. In the present case, it has been established that the platform security objectives set out in the Company's Rules could have been achieved by other means that did not require the collection of additional personal data from the Applicant (telephone number)[5], and therefore the Inspectorate has no grounds to assess such data processing as objectively necessary within the meaning of Article 6(1)(b) of the GDPR. The right

[1] Guidelines, point 25.
[2] Clause 1.5 of the Rules also provides that a person's account may be confirmed by using Facebook, Google accounts, or other methods that the Company may apply at its discretion.
[3] Guidelines, point 30.
[4] Point 16 of the Guidelines states that both the purpose limitation principle and the data minimisation principle are particularly relevant in cases where contracts are concluded for online services, as such contracts are generally not individually negotiated. Due to technological progress, data controllers are able to collect and process more personal data than ever before. This entails a significant risk that data controllers may seek to incorporate general data processing terms into contracts in order to collect and use as much data as possible, without properly specifying the purposes for such processing and without considering the possibility of complying with data minimisation obligations.
[5] An account could have been verified using other personal data already held by the Company (for example, email).

of the Company under the Rules to require the Applicant to provide her telephone number "for security reasons" also cannot, in itself, justify the proper application of Article 6(1)(b) of the GDPR.[6]

Secondly, when assessing whether Article 6(1)(b) of the GDPR is an appropriate legal basis for data processing where an online service is provided under a contract, consideration should be given to the specific objective, purpose or function of the service. [7] In the opinion of the Inspectorate, the primary purpose of the contract being performed, where the Company is acting as the operator of an e-commerce platform, is to provide individuals with the possibility to operate on the platform as buyers/sellers. Although the Inspectorate agrees that an important part of the proper functioning of such a platform is the security of the platform and the accounts within it, the assurance of this security cannot be based on the performance of the contract with the data subject. This conclusion of the Inspectorate is directly confirmed by the Guidelines, which, when discussing specific cases of the application of Article 6(1)(b) of the GDPR, in the section on "Data processing for fraud prevention purposes,"[8] state that such data processing will likely encompass more than what is objectively necessary to perform a contract with the data subject.[9]

This practice is also followed by the EDPB, which in its binding decision No. 5/2022 of 5 December 2022[10] among other matters, examined whether WhatsApp IE could rely on Article 6(1)(b) of the GDPR for processing data of subjects for "security" purposes. The EDPB indicated that if the Irish supervisory authority does not find that WhatsApp IE violated Article 6(1)(b) of the GDPR, this provision essentially becomes meaningless and theoretically any collection and reuse of personal data related to the performance of a contract with the data subject becomes lawful. Accordingly, the EDPB concluded and agreed with the arguments of the relevant supervisory authorities that the data processing was not objectively necessary[11] for ensuring security functions and was not an essential or principal part of such a contract[12].

Although the Company additionally emphasises in the Reply that this measure (telephone number verification) is intended, among other things, to implement the requirements of Article 31 of the GDPR and ensure the security of personal data, the aim to ensure compliance with GDPR requirements in the context of the Applicant's Complaint cannot justify the proper application of Article 6(1)(b) of the GDPR. [13]

Finally, the Inspectorate notes that, on the one hand, as seen from Clause 1.5 of the Rules, during registration on the Company's platform the data subject (including the Applicant) is required to provide a username (pseudonym), email address, and password, while the provision of a telephone

---

[6] Such a position is also observed by the EDAV. Point 27 of the Guidelines states that merely stating or referring to data processing in a contract is not sufficient for the processing to be based on Article 6(1)(b). To be "necessary for the performance of a contract," one certainly needs more than just the terms of the contract.

[7] Guidelines, point 30.

[8] Considering that the Applicant's account verification using her telephone number was invoked because a "suspicious login" was detected (Company's Reply, p. 1), the purpose of such data processing was, among other things, to prevent possible fraud by gaining unauthorized access to the Applicant's account.

[9] Guidelines, point 50.

[10] Internet link to the EDPB decision (in English): https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-52022-dispute-submitted_en

[11] Points 121, 122 of the decision.

[12] In point 118 of the decision, the EDPB concluded that the primary purpose for which a user uses WhatsApp services is to communicate with other users.

[13] Point 50 of the Guidelines clarifies that the processing of personal data strictly necessary for fraud prevention purposes may be a legitimate interest of the data controller and thus may be considered lawful if the data controller meets the specific requirements of Article 6(1)(f) (legitimate interests). Moreover, the legal basis for such data processing may also be Article 6(1)(c) (legal obligation). Accordingly, if the Company partially bases data processing on the purpose of ensuring compliance with Article 31 of the GDPR, the Company should be able to demonstrate compliance with the provisions of Article 6(1)(c) of the GDPR (processing data is necessary for compliance with a legal obligation to which the controller is subject).

number is not a necessary condition to begin using the services provided by the Company. On the other hand, in the Reply the Company states that telephone number verification is carried out for the purpose of fraud prevention, platform and its members' security assurance, and that in the Applicant's case such verification procedure was initiated upon detecting a suspicious login. Accordingly, the Inspectorate considers that without objective data as to whether the telephone number entered during verification belongs to the platform account user at all[14], the processing of telephone number data to ensure the security of such an account essentially loses its purpose.

In summary of the above, it is concluded that the processing of the Applicant's personal data (telephone number) in the context of the Complaint could not have been based on the lawful processing ground established in Article 6(1)(b) of the GDPR, as such processing was not objectively necessary for the performance of the contract with the Applicant. On other grounds established in Article 6(1) of the GDPR, the Company did not base the processing of the Applicant's personal data (telephone number), and therefore the Inspectorate does not comment further on them (Article 5(2) of the GDPR). Accordingly, the Complaint is recognised as justified.

Regarding the imposition of corrective measures on the Company

Article 31(2) of the Law on Legal Protection of Personal Data of the Republic of Lithuania (LLPPD) provides that where a complaint or part thereof is recognised as justified, the Inspectorate shall issue instructions, recommendations, and/or apply other measures provided for in 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 regarding personal data processing and/or privacy protection.

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)(d) of the GDPR provides that each supervisory authority has the power to require the data controller or data processor to bring processing operations into compliance with the provisions of this Regulation, in certain cases by a specified procedure and within a specified period.

In the present case, having established that the Company unlawfully processed the Applicant's personal data (telephone number) on the basis of Article 6(1)(b) of the GDPR, it is concluded that the said data are processed unlawfully, and accordingly the Company is obliged to delete this data

Furthermore, considering that it is likely that the Company processes (and intends to process) other data subjects' data (telephone numbers) under similar circumstances and in order to ensure the ongoing compliance of the Company's data processing activities with the GDPR provisions, the Company is instructed to ensure that data subjects' data (telephone numbers) are not processed for the purposes of fraud prevention, platform, and its members' security assurance on the basis of Article 6(1)(b) of the GDPR.

Pursuant to the foregoing, Article 31(1)(1) and Article 31(2)(1) of the LLPPD, Article 58(2)(d) and Article 60(7) of the GDPR, the Inspectorate

[14] Since the Applicant did not provide her telephone number during platform registration, the corresponding verification or confirmation procedure to check whether the telephone number entered matches the Applicant's is objectively impossible.

hereby decides:

1. To recognize the Applicant's Complaint as well-founded.
2. To provide the Company with instructions within 1 (one) month from the date of receipt of this decision:

2.1. To delete the Applicant’s telephone number data;

2.2. To ensure that data subjects’ telephone numbers are not processed for fraud prevention, platform, and its members’ security assurance purposes on the basis of Article 6(1)(b) of the GDPR.

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]