REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

All SA's

Our 23.05.2025 No. 2.1.-1/24/108-224-10

ARTICLE 60 FINAL ADOPTED DECISION
Termination of the proceedings

The Lithuanian Data Protection Authority forwarded to the Estonian Data Protection Inspectorate (the Estonian DPI) the request of the Lithuanian Consumers Alliance (hereinafter the Alliance). According to the request, the Alliance has identified certain violations of personal data protection rules by [redacted], [redacted] and [redacted] in connection with the processing of personal data in Lithuania.

Under Article 77(1) of the General Data Protection Regulation (GDPR), every data subject has the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data concerning him or her infringes the GDPR. The request was made by the Alliance, which in this case does not have the right of representation of any specific data subject. However, the Estonian DPI initiated proceedings[1] to examine the facts set out in the request. As the controller is [redacted] (hereinafter [redacted], the Controller), the Estonian DPI submitted inquiries and a proposal to the Controller.

Circumstances set out in the request

The Alliance's request is motivated by the fact that there are more and more cases of financial fraud in Lithuania, where consumers' bank accounts are illegally debited for [redacted]'s services. Given that, in Lithuania, pursuant to Article 34 of the Law on Payments, the consumer is obliged to protect personalised security data upon receipt of a payment instrument, the Alliance analysed the personal data processing documents published by [redacted] concerning the processing of the consumer's payment card data.

The Alliance considers that the Controller does not fulfill the notification obligation set out in Articles 12-14 of the GDPR and that there are the following shortcomings in the processing of payment card data.

The Alliance is of the opinion that it is difficult for the average consumer to understand which documents are intended for which service users from the privacy notices disclosed by the Controller, for example, which privacy notices are directed at taxi service user and which are addressed to [redacted] Drive service user. Therefore, the Alliance requests that data subjects be informed about the processing of personal data in a clear and comprehensible manner (Articles 13 and 14 GDPR) by structuring the privacy notices of all [redacted] services according to the nature of the services provided, so that it is clear to the user which personal data is processed and how it is

[1]The Estonian DPI commenced supervision proceedings on the basis of Section 56(1) and (3)(8) of the Personal Data Protection Act.

processed after the purchase of the relevant [redacted] service.

It is not clear from the privacy notices whether [redacted] transmits the user's payment card data to drivers as part of the provision of the ride-sharing service. The Alliance notes that the Passengers and Riders Privacy Notice states that 'A passenger's personal data is only disclosed to drivers providing a ride-hailing service when they provide a ride-hailing service using the [redacted] app, in which case the driver sees the passenger's name, phone number (in some countries, the phone number is masked) and geolocation data.' However, it remains unclear which entity of the Controller stores and uses the passenger's payment card data to collect money for the services provided by [redacted] or the drivers.

The Alliance considers that there is no publicly available privacy notice for buyers of the [redacted] Drive service. The Alliance therefore requests that a Privacy Notice for [redacted] Drive be prepared and made publicly available containing the information set out in Articles 13 and 14 GDPR in a clear and comprehensible manner.

The Alliance notes that the Privacy Notice addressed to the drivers states the following: 'Financial information relating to transport services is not considered personal information as drivers provide a service on an individual economic activity basis' The Alliance considers that such a conclusion does not meet the definition of personal data in Article 4(1) of the GDPR, since personal data are any information relating to an identified or identifiable natural person, irrespective of whether the natural person is engaged in an individual economic activity or not.

The CEO of [redacted] Lithuania has publicly stated that the application of the Controller does not store the card data of the users and is not responsible for the security of these data. The CEO also stated that third parties are responsible for the security of payment card data. Such a statement contradicts what is stated in the privacy policy of the Controller and creates confusion for data subjects.

The Privacy Notice for Passengers and Riders states that the Controller processes, inter alia, 'payment information, such as the amount charged and the payment card used'. The Controller does not specify in the privacy notices which payment card data it collects and stores. The Alliance requests that privacy notices specify that the type of payment card, number, expiration date and CVV code are processed. A specific list of these data is very important for the data subject because, following the disclosure of the payment card security code to a third party ([redacted]), according to Article 34 of the Lithuanian Law on Payments, the consumer himself is obliged to take care of the security of such personal data and to know the persons holding the previously transmitted payment card security code.

The Alliance is of the opinion that [redacted] will not disclose to data subjects in a privacy notice for what purpose and to which third party the Controller will transfer payment card data. The Alliance considers that it is important for data subjects to know in advance to which entity their payment card personal data will be provided, who will be the controllers and processors of such personal data and to which third parties such personal data will be transferred. The Alliance considers that users have not given their consent, nor is there any other legal basis for transferring their payment card data to other third parties, which [redacted] calls 'partners'.

The Alliance shall request the supervisory authority to oblige the personal data controller(s) to carry out, as soon as possible, an independent audit of a possible personal data breach of consumer payment card data and to provide the results of that audit to the Alliance and all relevant customers (data subjects).

Clarifications by the Controller

The Controller provided the Estonian DPI with links to privacy notices applicable to different users in Lithuania and explained that [redacted] website has a special website dedicated to data protection (in

different languages for the respective markets at: [redacted]), designed to be user-friendly and transparent. The Controller explained that the [redacted]'s data protection website is easily accessible via a link at the footer of the [redacted] website. The data protection website is divided into different sections for each service (Rides, Micromobility, [redacted] Drive, etc.). Users can choose their service type and will then be redirected to the privacy notices applicable to the specific [redacted] service. The Controller believes that this structured approach is in line with the requirements of the GDPR as it allows for clear and accessible information tailored to the specific service of the user. In addition, the Controller indicated that the privacy notices will be reviewed and updated to make them even more user-friendly. The updates also include the design of the Privacy Notice to ensure that the information is presented in a more accessible and understandable way. The revised Privacy Notice is expected to be published in Q2 2025 (i.e. in all countries where [redacted] operates, including Lithuania). Privacy notices are harmonised across countries to ensure that transparency requirements are uniformly guaranteed for all users. The Controller pointed out the updates to the various privacy notices addressed to Lithuanian data subjects that have taken place during the course of the present proceedings.

The Estonian DPI asked the Controller to explain why two different privacy notices have been created for passengers. The Controller explained that the co-existence of both the Privacy Notice for Passengers and the Privacy Notice for Passengers and Riders was temporary, and the situation was remedied by the publication of the Global Privacy Notice on Micromobility[2].

Regarding the link to the data protection website in Lithuania's Terms and Conditions of the [redacted] Drive[3], the Controller stated that there was an incorrect link in the past. The error was corrected after noticing it, which is why the Terms and Conditions of the [redacted] Drive now contain the correct reference.

As regards the transmission of payment data, the Controller explained that although drivers receive certain personal data necessary for the provision of the transport service (such as the pick-up and destination address, passenger name and average rating), they do not contain payment data. The [redacted]'s Global Privacy Notice for Passengers[4] states that drivers do not receive any payment details from passengers. The transmission of data for [redacted] services follows the same logic in all EU countries, i.e. drivers do not receive payment data from passengers in any EU country. The Controller described the processing of payment data to the DPI.

[redacted] stated that, based on the requirements laid down in the GDPR and also on normal market practice, it is necessary to specify the categories of personal data to be processed. In line with this requirement, the Global Privacy Notice for Passengers explains what 'payment data' is and how it is processed. In particular, Section 3, entitled 'Personal data you have shared with [redacted]', states: 'We collect information about your payment methods, including payment card type, bank name, bank account number, bank account sort code, related payment confirmation information and transaction history on the [redacted] platform.' In addition, information about the purposes of processing payment data and the legal basis on which [redacted] relies is provided. The Controller further stated that in order to ensure consistency and clarity in all [redacted] Privacy Notices, similar wording will be introduced in other relevant Privacy Notices, as appropriate, in the context of its proposed updates. The Controller considers that this approach will provide [redacted] users with a clear overview of the payment card data being processed.

With regard to the privacy notice for drivers, the Controller agreed that the specific wording ('Data related to the cost of the ride service is not personal data because drivers provide services in the course of their economic and professional activities') is not in line with the privacy notices applicable to drivers of other markets. The Controller removed this section from the Privacy Notice for Drivers. [redacted] confirmed that it treats payment-related data as personal data and that the list of

[2] Available: [redacted]
[3] Available: [redacted]
[4] Available: [redacted]

personal data processed has been updated to explicitly include payment data.[5] The Controller explained how the payment data description is planned to be reflected in the updated Privacy Notice for Drivers in order to further improve transparency.

The Estonian DPI asked the Controller to clarify whether [redacted] had any personal data breaches in 2023 that could be related to the financial fraud in Lithuania mentioned in the Alliance's request. The Controller explained that, following thorough internal controls and investigations, [redacted] has no information or evidence that any personal data breaches or personal data leaks occurred in their systems in 2023 in relation to the alleged financial fraud in Lithuania mentioned in the Alliance's request. In the absence of information on affected data subjects, [redacted] is unable to verify whether the specific user accounts have been compromised in the manner referred to in the request.

[redacted] considers the security and integrity of information systems and personal data to be extremely important. For this purpose, [redacted] the potential weaknesses of the Controller's systems are rigorously assessed, and it is ensured that [redacted]'s protective measures remain robust against unauthorized access, data misuse, and potential data leaks.

The position of the Estonian Data Protection Inspectorate

1. The processing of personal data must be carried out in a transparent manner (Article 5(1)(a) GDPR). Article 12(1) GDPR provides that the controller shall take appropriate measures to provide the information referred to in Articles 13 and 14 to the data subject in a concise, clear, intelligible and easily accessible form, using clear and plain language. When applying the principle of transparency, it must be taken into account that the data subject is able to determine in advance the scope and consequences of the processing and would not be surprised at the subsequent use of their personal data.

2. Thus, one element of the principle of transparency is 'easily accessible information', which means that the data subject should not look for information, but should immediately be able to see where and how that information can be accessed. The Working Party on Data Protection has recommended that when the controller operates a website, it should use layered data protection terms, which allow website visitors to navigate to the specific aspects of the data protection terms that interest them the most.[6]

3. In its request, the Alliance indicates that the documents by which Lithuanian data subjects are informed of the processing of personal data are available on the website [redacted] and that it is difficult for the data subject to find the right privacy notice. In the opinion of the Estonian DPI, the website referred to by the Alliance is not the main place where data privacy notices are available. The Controller has created a separate data protection notice page on its website [redacted], which is accessible via the link at the footer of the [redacted] website. The Privacy Policy website is divided into different sections for each service. The data subject can choose the type of service, after which the data subject will be directed to the privacy notices applicable to the service. Thus, the Controller has taken a layered approach in providing data subjects with the information required by Articles 13 to 14 of the GDPR. The data subject does not need to search for the privacy notice within the terms of use. In the opinion of the Estonian DPI, [redacted]'s privacy notices are structured according to the service used and the respective privacy notices are easily accessible for the data subject, i.e. the data subject can reasonably understand how to reach the privacy notices on the website of the Controller and which privacy notices are aimed at the user of the ride-sharing service, for example. It is common

[5]The privacy policy applicable to Lithuanian drivers is available at: [redacted]

[6]Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679, WP 260 rev 01, 11 April 2018, p. 11, p. 8.

practice to provide a link to the privacy policy in the footer of the website. As regards the requirement of comprehensibility, the Estonian DPI also takes into account the Controller's confirmation that the privacy notices will be updated to make them even more user-friendly.

4. The Estonian DPI takes into account the confirmation from the Controller that the link referring to the data protection website within Lithuania's Terms and Conditions of the [redacted] Drive was incorrect and it was corrected after being noticed. Therefore, the correct link is now in Lithuania's Terms and Conditions of the [redacted] Drive, and it is also possible to reach the data protection content page through the general terms and conditions.

5. In its request, the Alliance indicates that the Controller does not specify in the privacy notices which payment card data it collects and stores. The Estonian DPI notes that Article 13 GDPR does not require the controller to provide information on the categories of personal data concerned. Such information must be provided where the personal data have not been obtained from the data subject (Article 14(1)(d) GDPR). Therefore, the GDPR does not require the controller to include information in the privacy notice about the categories of personal data obtained from the data subject. However, [redacted] has provided information about payment data in its privacy notices and has agreed to specify the payment data being processed.

6. Furthermore, the Estonian DPI notes that the principle of transparency requires the controller to provide the information accurately as to its content, while at the same time ensuring that the information is presented to the data subject in an easily understandable manner. It may therefore be difficult to comply with the requirements of Article 12(1) GDPR, as the information provided in the data protection terms under Articles 13 to 14 GDPR must be accurate and at the same time simplified. The Working Party on Data Protection has pointed out that it is up to the controllers themselves to analyse how to prioritise the information to be provided to data subjects and what are the appropriate levels of detail and methods for providing the information.[7] Therefore, while taking into account that the GDPR does not require the controller to include information about the categories of personal data received from the data subject, the Estonian DPI is of the opinion that the degree of accuracy of the provision of information on payment data is a discretionary decision of [redacted] and, in the Estonian DPI's view, the Controller has not breached the requirements of transparency in providing information on payment data. In addition, the Estonian DPI notes that each data subject has the possibility, under Article 15(1)(b) GDPR, to submit a request for access to the Controller, allowing him or her to become acquainted with the personal data processed by the Controller in relation to him or her.

7. The Alliance notes that it is not clear from the privacy notices whether [redacted] transmits the user's payment card data to drivers as part of the provision of ride-sharing services. At the same time, the Alliance itself sets out the relevant section of the privacy notice, which sets out the personal data that the driver sees about the passenger in the course of providing the ride-hailing service and payment data is not included among these personal data. The Controller also confirmed to the Estonian DPI that drivers do not have access to passenger payment card data. Thus, the data subject can obtain information from the privacy notice about the personal data transferred to drivers in the course of providing the ride-hailing service and the payment card data is not included in these personal data.

8. The Alliance pointed out that the explanation in the privacy notice addressed to drivers, according to which "Financial information relating to transport services is not considered personal information as drivers provide a service on an individual economic activity basis",

[7] Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679, WP 260 rev 01, 11 April 2018, p. 34, p. 18.

does not meet the definition of personal data laid down in Article 4(1) of the GDPR. [redacted] agreed that the specific wording of the Privacy Notice for Drivers of Lithuania is inconsistent with the Privacy Notices applicable to Drivers of other markets and removed this section from the Privacy Notice. The Estonian DPI is of the opinion that financial data may be personal data if it is possible to identify a specific natural person directly or indirectly through such data. Namely, Article 4(1) GDPR provides that personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly. The expression 'any information' emphasises that the concept of personal data is understood as broadly as possible. The Working Party on Data Protection has clarified that the concept of personal data includes information relating to an individual's private and family life in the narrower sense, but also information relating to any activity of the individual, such as information relating to his employment relationships or to his economic or social behaviour. This therefore includes information on individuals, regardless of their position or category (consumer, patient, employee, customer, etc.).[8] Therefore, the Estonian DPI agrees with the position of the Alliance that financial data related to the travel services may be personal data, despite the fact that drivers provide services in economic and professional activities. The Estonian DPI takes into account that [redacted] has also agreed with the above-mentioned position and, on that basis, corrected the privacy notice addressed to drivers.

9. The Alliance pointed out that the Controller does not inform for what purpose and to whom [redacted] transfers personal data related to the payment card. Pursuant to Article 13(1)(e) GDPR, at the time of receipt of the personal data, the controller shall inform the data subject, where appropriate, of the recipients or categories of recipients of the personal data. The Working Party on Data Protection has clarified that the actual (named) recipients or categories of recipients of personal data must be provided. In line with the principle of fairness, controllers must provide the information on recipients that is most relevant to the data subject. Where controllers decide to provide categories of recipients, the information should be as specific as possible, indicating the type of recipient, industry, sector or subsector.[9] The Controller's privacy notice for passengers sets out the categories of recipients of personal data, including a reference to third-party service providers that offer payment processing. The Estonian DPI is of the opinion that the Controller has provided information about the category of recipient of personal data, indicating the service provider providing payment processing as a category. The Estonian DPI here takes into account that the information provided in the Privacy Notice must be accurate, but at the same time concise and simplified in order to avoid information fatigue for the data subject. The determination of the degree of accuracy is the responsibility of the controller (see point 6 of this Decision), and the GDPR does not require naming the recipients in every possible case. In order to obtain more specific information, the data subject has the right under Article 15(1)(c) GDPR to obtain from the Controller information on named recipients, i.e. more specific data on recipients.

10. According to Article 4(12) GDPR, 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Article 32(1) GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data. Pursuant to Article 32(2) GDPR, the assessment of the appropriate level of security shall take into account, in particular, the risks posed by the processing of personal data, in particular the accidental or unlawful destruction, loss,

[8]Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Adopted on 20 June 2007, WP 136, p. 6.
[9]Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679, WP 260 rev 01, 11 April 2018, p. 37.

alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11. The Estonian DPI asked the Controller to clarify whether and what [redacted] has done in its investigation of information systems in order to prevent unauthorised access to information systems, misuse of data and possible data leakage in connection with the financial fraud in Lithuania, which was mentioned in the Alliance's request. The Controller confirmed that it has carried out internal controls and investigations but has found no indications of personal data breaches or leaks of personal data in [redacted]'s systems in 2023 related to the alleged financial fraud in Lithuania mentioned in the request. In the absence of information on affected data subjects, [redacted] is unable to verify whether the specific user accounts have been compromised in the manner referred to in the request. In the opinion of the Estonian DPI, in the absence of specific information about a possible breach mentioned in the request, it is not possible to conclude with certainty that financial fraud has occurred as a result of a personal data breach committed by the Controller. In that regard, the Estonian DPI also takes into account the fact that an article in a newspaper referred to in the request states that the fraud involved a bank card that was not linked to the user's account.

12. Pursuant to Article 31 GDPR, the controller shall cooperate with the supervisory authority at its request in the performance of its tasks. The Controller has cooperated with the Estonian DPI and confirmed that it has carried out an investigation into financial fraud in Lithuania in order to identify a possible weakness in its information systems, but did not identify any breach. Therefore, no breach of security by the Controller has been identified, which would have resulted in financial fraud in Lithuania. In addition, the Controller has reviewed and updated the privacy notices to make them clearer also with regard to the processing of payment data. The Estonian DPI takes into account that data protection terms are a living document that is regularly reviewed and, if necessary, updated. **On the basis of the above, the Estonian DPI terminates the supervisory procedure.**

13. In its request, the Alliance also addressed the requirements of the Digital Services Act (DSA Regulation) applicable to the [redacted] platform. Since the Estonian DPI is not the competent supervisory authority for the DSA Regulation, this supervisory procedure does not concern the verification of compliance with the requirements of the DSA Regulation.

14. However, the Estonian DPI draws the attention of the Controller to the recommendation of the Data Protection Working Party to introduce layered privacy notices to link different types of information provided to the data subject in order to avoid information fatigue, rather than displaying all such information on the screen as a single notice. Layered privacy notices can help resolve the tension between integrity and comprehensibility, namely by allowing users to navigate directly to the part of the notice they want to read. Therefore, when updating the privacy notices, the Estonian DPI recommends adding links to the table of contents, which would allow the data subject to navigate more easily to the section that interests him or her.

This notice of termination of the supervision proceedings can be challenged within 30 days by submitting an appeal to the administrative court under the Code of Administrative Court Procedure[10].

Respectfully,

[redacted]
lawyer
authorized by the Director-General

[10] https://www.riigiteataja.ee/en/eli/ee/512122019007/consolide/current