REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FOR DATA PRIVACY AND FREEDOM OF INFORMATION
FOR INTERNAL USE
Holder of information: Data Protection Inspectorate
Date: 30.05.2025
Valid until the decision enters into force
Legal ground: Public Information Act § 35 cl 1 p 2

30.05.2025 nr 2.1.-1/23/1109-1754-1

Notice of reprimand and termination of the proceedings concerning the protection of personal data

The Estonian Data Protection Inspectorate (Estonian DPA or DPA) received a complaint from the Hungarian National Authority via the cross-border procedural system IMI that passengers are assessed through the [redacted] application service by the drivers after using the ride hailing. According to the complaint, passengers are not informed about the processing of their personal data, and the person cannot give consent. In the context of this, Estonian DPA agreed to be the lead supervisory authority and initiated supervision proceedings based on clause 56 (3) (8) of the Personal Data Protection Act.

THE COURSE OF THE PROCEEDINGS

The complaint was received by the Estonian DPA 03.12.2021 and in the beginning of 2022 the DPA made primary inquiries about the legal basis for the processing of personal data and duration of the storage of personal data.

The Estonian DPA was in the opinion that the controller did not have a legal basis for processing the personal data concerning ratings given to passengers by the drivers (rider ratings). Thus, the DPA issued a formal injunction on 17.02.2022 to suspend the processing of the data until the data controller has implemented measures in compliance with the General Data Protection Regulation (GDPR) and to delete all personal data related to rider ratings. The data controller replied to the injunction, confirming that it complied with the injunction and provided further information. **(DPA's injunction – Annex 1, [redacted]'s initial response – Annex 2)**[1]

Pursuant to GDPR Article 60(3), the DPA published the first version of the draft decision on IMI on 20th February 2023, but several comments and objections were raised. The Estonian DPA agreed with the comments of the other supervisory authorities and continued the supervisory proceedings against [redacted].

In autumn of 2023 in the continued proceedings, it was found that the data controller had not complied with the initial injunction made on 17.02.2022. It was found out that [redacted] had not deleted all personal data relating to rider ratings and had not stopped the processing of personal data. Thus, the DPA issued a renewed warning, but because some time had passed, it set out a new deadline. **(DPA's warning – Annex 3)**

[1] All annexes are machine translated from Estonian to English

On 17.10.2023 (registered in our systems 18.10.2023) [redacted] and [redacted] data protection officer notified the Estonian DPA by email, during answering an inquiry, that since 01.01.2022 the controller for the data processing activities in question is [redacted] (hereinafter [redacted]). Since the board for this entity is also located in Estonia and all decisions concerning data processing activities are made in Estonia, the DPA deduced that it was still the leading supervisory authority in this case. **(Notification to the Estonian DPA – Annex 4)**

The controller then disputed the renewed warning and 17.02.2022 injunction in the Administrative Court. The controller also notified that it had stopped all personal data processing activities in relation to rider ratings from 31.10.2023.

The court accepted the dispute but suggested a compromise and thus the Estonian DPA and [redacted] started negotiating an agreement to settle the issue out of court. The final agreement was achieved in spring 2024 after which [redacted] withdrew their complaint from the court. The Estonian DPA agreed to modify the original injunction (detailed explanation is brought out in the following sections) by requesting the deletion of data older than three years and updated the initial order as regards to the reasoning related to the legal basis and transparency principle requirements. **(DPA's updated injunction – Annex 5).**

In spring 2024 the controller notified the DPA that it had complied with the renewed injunction – it had met all requirements to continue processing personal data under the legal basis of legitimate interest, updated its privacy policy and in-app information and deleted all data older that three years. The Estonian DPA allowed the controller to continue processing personal data in relation to rider ratings from 25.04.2024. **([redacted]'s notification – Annex 6; DPA's response – Annex 7; Court ruling – Annex 8)**

During the whole proceedings, the Estonian DPA made several inquiries in the period of January 2022 until December 2024 to get an overview of personal data processing activities in the [redacted] application. The Estonian DPA also met with the controller several times during these proceedings.

On 01.11.2024 the Estonian DPA published a revised draft decision but was met with extensive comments from the French SA. In the period of November 2024 until the end of January 2025, the Estonian DPA and French SA communicated in concern to the revised draft decision and the French SA made several suggestions that were considered to update and enhance the reasoning of the revised draft decision. The conclusion and decision to reprimand and end the proceedings were not changed.

POSITION OF THE ESTONIAN DATA PROTECTION INSPECTORATE

A. The legal basis of personal data processing

According to Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), "personal data" means any information relating to an identified or identifiable natural person, in particular name, personal identification number, location information; the physical, physiological, and economic characteristics of the person etc. The ratings given to passengers hailing a ride through [redacted], which are then connected to their account via an average rating are also considered to be personal data.

The controller at first argued that the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract according to article 6 (1)(b) of GDPR. The Estonian DPA did not agree with this reasoning.

Under Article 6(1)(b) GDPR, it is possible to process personal data only if the processing of personal data is objectively necessary for the achievement of the purpose set out in the contract or for the performance of a specific contractual obligation. However, as regards the assessment (profiling) of passengers after a journey during the provision of taxi services, it cannot be a matter of ensuring the performance of a contract within the meaning of the GDPR, i.e. the contract can be carried out without assessing the passengers. Similarly, in other areas of life – for example, stealing from shops is not allowed, but this does not mean that in order to ensure the performance of the contract, it can be necessary to add an assessment to each customer showing how trustworthy a person is to visit a shop and shop there.

In the opinion of the Estonian DPA, it is possible to rely on certain assumptions in the case of profiling only based on Article 6(1)(f) GDPR (legitimate interest) and only if it is proportionate. Therefore, the assessment of passengers may in theory be necessary for the legitimate interests of the data controller and/or the drivers. However, this requires a proper legitimate interest assessment (LIA) to be carried out, including additional safeguards, e.g. easy access for the data subject to the assessments made of him/her and the person making the assessment, and easy access to object to the assessment. During the proceedings, the controller agreed that the processing should be based on legitimate interest.

One the concerns raised in relation to the LIA was that the Estonian DPA could not verify the balancing test of rights and interests described in the original LIA (version one submitted to the DPA in march of 2022 and version two in autumn of 2023), as it did not contain a clear overview of how the result would be achieved and contained a number of inconsistencies with actual data processing and different sources of information (e.g. privacy policy and information in [redacted] application). The data controller must first be able to justify that the legitimate interest being weighed is legitimate, sufficiently clear and specific. Here are examples of problems that the DPA found in the original LIA versions:

- The description of how the overall rating of the passenger is formed is unclear. The analysis mentioned that the calculation takes place in the last 40 estimates calculation of the average. In another place it is mentioned that the aggregated estimate does not take into old data, but only data from the last three months. The [redacted] application describes that estimations made during the last year are considered in the calculation of the overall score. Consequently, it is unclear which procedure applies to the development of the overall assessment of the passenger.
- The analysis of legitimate interest does not indicate for exactly how long the results of specific assessments will be retained. Also, whether and in what circumstances specific assessments are erased.
- The analysis mentions that the data subject, i.e. the passenger, can obtain more precise information about data processing and provide explanations through customer support. However, there is neither in the application nor in the data protection conditions, information where it is possible to get acquainted with legitimate interest assessment. It is also not known whether the data subject can object to a specific rating or an overall rating.
- It has not further explained what a negative overall score is and what are the specific

consequences for such an assessment to the data subject.

- In the original version of the LIA, it turned out that the threat to the safety of driver's property or person is on the same level everywhere but considering that [redacted] operates in many EEA countries, the level of threat to the [redacted] platform and [redacted] drivers may vary depending on the region. [redacted] must be able to demonstrate, through real-life examples, that a legitimate interest is not merely speculative.
- It is unclear whether data processing is mandatory for the driver. At the meeting [redacted] stated that it was voluntary, but the following analyses of legitimate interest state that it is mandatory data processing that the driver must carry out after the end of the journey.
- The data controller had to better explain what the alternative options were and why they were not proportionate regarding the respective measure (assessment of passengers). The assessment must clearly show why a particular measure is appropriate, necessary and moderate. For example, it is possible for the driver to take additional measures to ensure his or her safety in the car (calling the police or an ambulance). However, this part was not included in the first versions of the analysis.
- The section describing the rights and interests of the data subject was incomplete. The DPA did not agree that warnings would not produce legal effects concerning the data subject or significantly affect him or her. For example, in the case of a negative assessment, [redacted] directs the data subject to take additional steps (i.e. directs him/her to using a review service). In addition, a negative assessment also has an impact on the possibility for the data subject to subscribe to the service (drivers may refuse his/her travel request). Thus, the description of the rights and interests of the data subject should have been as comprehensive as the description of [redacted]'s own interests.

The controller submitted multiple versions of a legitimate interest assessment to the Estonian DPA, which were then reviewed. In spring 2024 the controller provided a thorough and complete legitimate interest analysis demonstrating the existence of a legitimate interest legal basis. This includes covering all important aspects of the GDPR, such as how data is collected and analyzed, how long assessments are stored, what additional safeguards are taken, how the data subject can object and how the data controller handles objections and other GPDR requests. In addition, the previous differences between actual data processing and the text contained in the analysis had been resolved. For example, the retention periods were initially not the same in analysis and in practice, which led the DPA to question which retention period was correct. The final version of the LIA (automated machine translation) is added to this revised draft decision as a reference. (**[redacted]'s final LIA – Annex 9)**

Here is a detailed overview of the changes that [redacted] made:

- Refined the purpose for processing personal data

Expanded objectives to highlight trust, safety, and market stability. Emphasized unique risks (e.g., night-time rides, intoxicated passengers) and demonstrated alignment with [redacted]'s, drivers', and passengers' interests.

- Necessity assessment

Compared alternative measures (e.g., law enforcement involvement, simplified rating systems) and justified the five-star rating as the most effective for ensuring balanced, detailed feedback.

- Data minimization and retention

Defined specific retention periods (Passenger ratings: 3 years as in 365 days + 2 years). Justified that the retention period is based on necessity for investigations, legal claims, and behavioral trends.

- Transparency and data subject rights

Enhanced the privacy notice with clear explanations of the rating process. Planned in-app features to inform passengers about rating calculations, retention, consequences and contestation rights.

- Privacy safeguards

Implemented privacy-by-design measures:

a. Restricted individual rating visibility to essential staff
b. Limited the timeframe for drivers to view aggregated average ratings
c. Mitigated emotional impact by offering customer support for contesting ratings and ensuring private rating mechanisms.

- Impact assessment and mitigation

Analyzed potential negative effects (e.g., anxiety, ride refusals) and introduced safeguards like rating contestability and limited influence on service accessibility, concluding minimal impact to the data subject.

- Legal compliance

Strengthened Article 6(1)(f) GDPR legal basis by referencing case law and ruling out consent or contractual necessity as viable alternatives. Demonstrated adherence to accountability, proportionality, and necessity principles.

B. Transparency of personal data processing

The Estonian DPA also criticized compliance with the principles of fairness and transparency (Article 5(1)(a) GDPR) and specifically the requirements in GDPR articles 12-14. In this context, it is important to look at how compliance with the principle of transparency is ensured in practice. During the proceedings, the DPA found that the obligation to provide information had not been complied with in respect to the data subjects.

The transparency principle in the GDPR ensures that individuals are informed about how their personal data is collected, used, stored, and shared. It underlines that data controllers must process personal information in a way that is open and understandable to data subjects. Transparency is essential, because it enables individuals to make informed choices about their data and exercise their rights under GDPR, such as the right to access, rectification, or erasure. This principle is achieved by providing clear, accessible and straightforward information at the point of data collection, in this case through the privacy notice and [redacted] application.

Examples of infringements of the transparency principle identified by the DPA:

1. The privacy policy lacked the necessary granularity and specificity required for key aspects of data processing, including automated decision-making and data-sharing practices.
2. The privacy policy did not offer users clear and accessible methods to exercise their rights under GDPR, particularly concerning objections, rectifications, or automated decisions.
3. The explanation about the rider rating was partly reflected in the [redacted] application by clicking on the aggregated assessment, but to ensure the transparency principle of the GDPR, the information provided to data subjects must reflect all the requirements addressed in article 12-14 of the GDPR. This must firstly be done in the privacy policy. It was found during the investigation that the correct and up to date information was not published in the [redacted] mobile application as well as on the official webpage. [redacted] prioritized updating the information on the app or through blog posts, but did not update the privacy policy accordingly.
4. Legal bases for personal data processing were not sufficiently explained or justified (Article 13(1)(c)):

    a. [redacted]'s privacy policy did not specifically mention that assessments are made of passengers. It contained the following sentence: *We uphold and promote standards: We collect data from driver feedback on travel statuses, time and passenger ratings in order to enhance user security, improve compliance with our terms and conditions and ensure that we provide a high-quality and enjoyable service to everyone.*
    b. There were generic references to "legitimate interest" without specifying or justifying the underlying interests.
5. Lack of clarity on timelines for responding to data subject requests (e.g., objections, data access, or rectification requests).
6. Insufficient transparency regarding recipients or categories of recipients (Article 13(1)(e)):
    a. Unclear who might access or process rider ratings and behavioral feedback.
7. Lack of clarity about data retention (Article 13(2)(a)):
    a. Retention periods for key data categories, including rider ratings, were not disclosed or adequately explained.
8. Inadequate explanation of data subjects' rights (Article 13(2)(b) and article 14(2)(c)):
    a. The right to object under Article 21 was mentioned but not accompanied by actionable details or accessible procedures. Thus, it was not clear how exactly the processing of objections was ensured, including whether there is a possibility for the data subject to suspend the processing of personal data (i.e. the data subject could not be assessed).
9. Failure to disclose data sources (Article 14(2)(f)):
    a. No information was provided on the sources of inferred or third party-provided data.

As of 10.04.2024 the controller uploaded the final version of the privacy policy that addressed all concerns raised during the proceedings and made changes in the [redacted] application. The Estonian DPA finally concluded that the transparency requirements had been fulfilled, and the continuance of the data processing activities may be carried out. [2]

The changes made in relation to the transparency principle:

1. The policy now provides a more detailed explanation of how rider ratings are calculated, stored, and used. Specifically:
    a. It explains that ratings are averaged over a 365-day period and displayed to drivers before they accept a ride.
    b. Clarifies that ratings influence potential warnings or temporary account suspensions, introducing a more structured approach to managing low ratings.
2. The policy explicitly mentions that automated systems are used to monitor rider ratings.
    a. It explains that warnings are automatically issued if the rating drops below a threshold, and if no improvement occurs, an automated suspension is applied. This reflects GDPR requirements for transparency in automated decision-making.
3. Detailed information is given on a feature that allows riders and drivers to block future interactions after giving a 1-star rating. This feature wasn't mentioned before.
4. The policy specifies that while drivers see the rider's average rating, individual ratings and feedback are kept private between [redacted] and the rider, emphasizing stricter data confidentiality.
5. The policy links the processing of rider ratings directly to [redacted]'s legitimate interest as a legal

[2] The updated version of the privacy policy is available here: [redacted]

basis, highlighting their aim to ensure platform safety, trust, and quality.
    a. Included are examples of how this supports operational goals, such as preventing unsafe or negative rider-driver interactions.
6. The newer version includes a defined process for handling low rider ratings:
    a. Warnings are issued automatically when the rating falls below a specific threshold.
    b. Temporary suspensions may occur if no improvement is seen within a set period.
7. The updated policy now elaborates on automated systems used in matching riders with drivers, fraud prevention, and account suspension, including mechanisms for user recourse against automated decisions.
    a. The policy explicitly explains the circumstances under which data subjects can object to the processing of their personal data. This includes objections to processing based on legitimate interests, automated decision-making, and profiling.
8. Clear instructions are provided for how users can submit objections through contact channels such as the Data Protection Officer (DPO) or in-app support.
    a. Users are informed that in cases of automated decision-making with significant effects, they can request manual review or human intervention.
    b. The updated policy offers multiple clear communication options for submitting objections, including through the in-app support menu or directly contacting the privacy team via email. These channels ensure that users can exercise their Article 21 rights effectively.

C. Problem of previously collected data

One of the problems that arose during the proceedings was that the data controller initially relied on the legal basis for the performance of the contract and then changed it and said that they were relying on a legitimate interest. In doing so, the data controller sought to argue that the previous data processing was legal and therefore it was necessary to preserve all collected personal data in relation to rider ratings (they wanted to keep data for the full account validity + 1 year after account closure).

[redacted] argued that if the DPA finds that the processing of personal data was carried out on an incorrect legal basis, this cannot lead to the automatic deletion of the personal data already collected, but the decision to delete must be an appropriate, necessary and proportionate measure to remedy the personal data breach. It also cited the Austrian Federal Administrative Court in case No W256 2227693-1/10E, saying:

- The Administrative Court did not share the interpretation of Article 29 of the Austrian DPA from the guidance material of the Working Party and from legal literature, according to which reliance on a different legal basis for the processing of personal data retroactively would be precluded.
- The principles of lawfulness, fairness and transparency in Article 5 of the GDPR must be considered separately, in the sense that a breach of the transparency requirements does not automatically result in an interference with the lawfulness of the processing of personal data, in so far as the opposite situation would result in the processor of personal data being required to erase all personal data collected.
- It is clear from the wording of Article 6(1) of the GDPR that the processing of personal data may be based on several legal bases which have equal weight in relation to each other. The Court also added that reliance on an alternative legal basis is not rendered unlawful by the fact that the data subject was not informed of the existence of alternative legal bases when the processing of personal data began.

It is the opinion of the Estonian DPA, that that recourse to a different legal basis retrospectively is not excluded, but for that to be the case, that legal basis must already have been set out in the Terms of Use/Privacy Policy. In the Austrian judgment, the controller relied solely on consent based on Article 6(1)(a). As the controller's terms and conditions did not rely on any other legal basis, the new legal bases raised by the controller could not be considered in the legal proceedings. In that case, there was a similar situation in which the applicant attempted retroactively to rely on the legal basis of legitimate interest, but they did not state this in advance in their terms and conditions, the data subject was not informed and there was no analysis of the legitimate interest.

In the current case legitimate interest was previously mentioned in the privacy policy. The problem being that it was not as direct and clear in wording as it is now in the new policy. Here are some examples from [redacted]'s old privacy policy:
Data on the use of transport services: such as travel status, times and drivers' assessment of your behavior.

We maintain and promote standards: We collect data on travel statuses, time and passenger ratings from driver feedback in order to enhance user security, improve compliance with our terms and conditions, and ensure that we provide a high-quality and enjoyable service to all. Customer support data and correspondence are collected for feedback and to resolve disputes and service quality issues.

3. Legal basis
We are permitted to use personal data in the manner described above if we have a valid reason for doing so. We always make sure that we have a good reason to process your data.

Personal data is usually processed in order to provide you with the services ordered through the [redacted] app. This means that in order to provide the service you have been promised and to comply with our terms and conditions, we will process your personal data to comply with these obligations.

In other circumstances, we generally process your personal data on the basis of a legitimate interest. Legitimate interests include our business interests in providing an innovative, personalized, secure and profitable service to passengers and partners, unless other interests override those interests. Our legitimate interests also include, for example, investigating and detecting fraudulent payments and other malicious activities, maintaining the security of our network and systems, and responding to suspected or actual crimes.

Bolt also pointed out from the Austrian decision that the fact that the data subject was not informed of the existence of alternative legal bases at the beginning of the processing of personal data did not render reliance on an alternative legal basis unlawful.

In the opinion of the Estonian DPA the lack of information to the data subject and the legality of the alternative legal basis are separate acts of GDPR infringement and the lack of information does not immediately mean that the alternative legal basis is unlawful. In CJEU Case C-621/22, and in point 41 of the judgment, the Court emphasized that the legitimacy of an interest should be assessed considering the applicable legal framework and all relevant circumstances. This means that while an interest does not need to be legally enshrined, it must operate within the bounds of the law and be evaluated on a case-by-case basis. So, for that alternative legal basis (legitimate interest) to be

substantively valid, the controller must have already pursued the legitimate interest and completed the necessary analysis. Separately, for any data processing relying on this basis to be lawful, the controller must also have brought this legal basis and the specific interests to the attention of the data subject.

It is also the opinion of the Estonian DPA, that there is no sufficient and concrete evidence to suggest otherwise, i.e. that [redacted] had no prior legitimate interest. [redacted] has pointed out previous statistics as to why ensuring security is an important and real reason for this processing activity (collection and storage of passenger ratings). [redacted] argued that the aim of data processing is for security purposes (to prevent future incidents; to provide a quick and easy way to give feedback to the service at the moment of the incident; to allow the client to unmatch so that they no longer encounter the unpleasant driver.). The purpose of safety was also previously mentioned in the old version of the privacy policy.

[redacted] provided to the DPA an initial LIA on 03.03.2022 and had proof that additional notifications about the data processing activities existed in the [redacted] application (under the aggregated rating).

In conclusion [redacted]'s personal data processing activities and the measures taken to protect the data subject rights did not fully comply with all the requirements of the GDPR at the time of the injunction, because the notification was not done correctly and the provided LIA had inconsistencies. However, this does not mean that [redacted] could not retroactively change the legal basis for data processing activities and bring its activities into compliance with the GDPR.

Considering all previously mentioned information and the cooperation on behalf of the data controller, the Estonian DPA came to the conclusion that in order to continue processing personal data (as well as previously collected data) on the basis of a legitimate interest, the data controller must have

(1) a properly formalized legitimate interest analysis proving that the controller has a legitimate interest in processing the personal data, and
(2) necessary notifications made to the data subject about the legal basis and processing activities.

The principles of legality, fairness and transparency laid down in the GDPR must be viewed as a whole, so as not to create a dangerous precedent in which the data controller can always rely on a new legal basis for previously collected data. It is therefore not an automatic right, but the data controller is obliged to justify how the legal basis applies to the data previously collected. It is the opinion of the Estonian DPA that in the end, the controller was able to provide sufficient evidence to justify the changing of the legal basis.

D. Data retention period

In section C it was mentioned that initially [redacted] argued in favor of the data retention period for as long as the data subject had an account in the [redacted] application plus one year after the deletion of the account. In the opinion of the DPA, this was not compliant with GDPR principles. Personal data must be kept no longer than necessary for the purpose for which it was collected (GDPR article 5(1)(e)). Once a user deletes their account, the original lawful basis for processing (e.g., contract performance or legitimate interest) no longer applies, unless the controller can demonstrate a compelling necessity for continued retention. Retaining rider ratings, comments, and other personal

data for one year after account deletion appears disproportionate unless there is a clear justification, such as handling disputes or legal obligations. Even then, the controller must show why this specific retention period is required and whether less intrusive measures, such as anonymization, could achieve the same goal. Additionally, [redacted] said that the data processing activity considers specific rider ratings for up to one year to calculate the aggregated rider rating. Thus, the initial retention period was unnecessarily long.

During the proceedings, the data controller changed their stance and explained that it is necessary for the data controller to retain the data related to rider ratings for three years from the moment they were collected. According to the data processor, this is justified by investigating fraud and safety incidents, resolving disputes and assisting passengers by providing explanations about passenger assessments and access requests. [redacted] also stated that the longer retention period can also be in the interest of the data subject, because this information is used for investigation purposes when reviewing unfair ratings given to a rider, when a rider makes a request for access or a complaint, or when a rider disputes their current average rating. In addition, the data controller wishes to protect itself against legal claims arising from contracts or claims arising from unlawful damage caused on the [redacted] platform. Under Estonian law, the limitation period for bringing such claims is three years.[3] Consequently, the Estonian DPA did not consider it proportionate to require the continued deletion of all passengers' assessments and agreed with the data controller's proposal.

Pursuant to Article 5(1)(e) of GDPR, the processing of personal data by the data controller must be based on the principle of storage limitation, according to which it would not be legitimate in this case to keep the data for more than three years. Upon submission of a valid legitimate interest analysis, the data controller has the right to store the data related to the assessments for a maximum of three years from the moment of their collection. Thus, the Estonian DPA requested the deletion of all previously collected personal data relating to the assessment of passengers, which had been collected at least three years ago.

[redacted] confirmed that as of 24.04.2024 all data older than three years and relating to rider ratings is deleted. [redacted] **confirmation – Annex 10)**

E. The reasoning for the outcome of the proceedings

In cross-border cases the Estonian DPA operates within the framework of the GDPR, which emphasizes cooperation and consistency among supervisory authorities. The Estonian DPA, like others, exercises its authority to ensure that controllers and processors comply with GDPR requirements. When a controller demonstrates compliance with the DPA's guidance and takes corrective actions to address identified issues, the DPA may decide to end the proceedings with a reprimand rather than impose an administrative fine. As is the case in the current complaint regarding [redacted]'s rider ratings.

This decision, to end the proceedings and issue a reprimand, aligns with the principle of proportionality under GDPR Article 83(1), which requires penalties to be appropriate to the nature, gravity, and consequences of the infringement. If the DPA concludes that the non-compliance was not severe or intentional, and the controller has voluntarily rectified the issues, a reprimand may be deemed a sufficient corrective measure. This approach allows the DPA to foster accountability and

[3] An Act on the General Part of the Civil Code § 146

encourage good practices without resorting to punitive measures when the circumstances do not warrant them.

It is important to note that in Estonia administrative fines are not directly applicable according to GDPR recital 151. Instead, fines must be determined through misdemeanor proceedings, which involve additional substantive and procedural requirements. These proceedings, similar to criminal proceedings, require the DPA to prove fault on the part of the controller, which entails a higher burden of proof. This is even though the GDPR sets out a cooperation obligation on the controller.

Furthermore, the procedural limitations of misdemeanor proceedings make them less effective in some cases. For instance, in Estonia, the statute of limitations for such cases is two years for infringements occurring before November 1, 2023, and three years for those occurring afterward. Given these constraints, pursuing misdemeanor proceedings in certain cross-border cases is often not a viable or efficient enforcement option.

The Estonian DPA's decision not to impose a fine reflects its focus on resolving issues cooperatively and efficiently. In this case, the proceedings were primarily aimed at putting an end to the GDPR infringement and the broader objective to protect the rights of a large number of data subjects. This approach is particularly relevant in cross-border contexts, where the DPA acts as a lead supervisory authority in collaboration with other EU counterparts. By issuing a reprimand, the DPA acknowledges the controller's efforts to comply while still ensuring that the infringement is formally addressed and documented. This balanced approach supports the GDPR's broader objectives of harmonizing data protection practices across the EU and promoting compliance without undue burden on entities that demonstrate good faith in rectifying their actions.

I hereby terminate the proceedings as the data controller has complied with all the proposals made by the Estonian Data Protection Authority.

In addition, I am reprimanding [redacted] on the basis of Article 58(2)(b) of the GDPR, because the processing operations have infringed the requirements of the GDPR (Article 5(1)(a) and (e), Article 6, Article 12(1) and (3), Article 13(1)(c), (d) and (f), Article 13(2)(b), Article 14(2)(c) and (g) and Article 21(4)).

This decision may be challenged within 30 days by submitting an appeal to an administrative court under the Code of Administrative Court Procedure[4]

Best regards

[redacted]
[redacted]
authorized by Director General

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