

Ridetechn International B.V.  
[ams-office@yandex-team.com](mailto:ams-office@yandex-team.com)

Yandex LLC, represented by HPP Attorneys Ltd.  
Att.: Attorney-at-law Kari-Matti Lehti  
[kari-matti.lehti@hpp.fi](mailto:kari-matti.lehti@hpp.fi)

Yango Norway AS  
Grønland 4  
0188 Oslo

Your reference

Our reference  
23/03080

Date  
07.08.2023

## **Advance notification – Yango – Transfers of personal data to the Russian Federation**

### **Background**

Yango is a taxi service that is used with the help of a mobile app. The service provider of the Yango application in the EEA is Ridetechn International B.V. (formerly Yandex.Taxi B.V.) based in the Netherlands. A case concerning the Yango application, and the lawfulness of transfers of personal data associated with that application, is the subject of a cooperation procedure between the European Data Protection Authorities. According to that investigation, personal data which relates to the users of the Yango application is being transferred to the Russian Federation. The lead supervisory authority in that case is assumed to be the Dutch supervisory authority, Autoriteit Persoonsgegevens.

In so far as this Decision concerns the processing of personal data by Yandex LLC, established in the Russian Federation, the Norwegian Data Protection Authority (“we”, “us”, “our”) is competent under Article 58 of the GDPR.

On 22 May 2019, the Office of the Finnish Data Protection Ombudsman requested Yandex Oy to provide information about which party is acting as the controller of personal data in relation to the Yango application. Yandex Oy responded to the request for clarification on 28 June 2019. According to its response, Ridetechn International B.V. (formerly Yandex.Taxi B.V.) based in the Netherlands is the service provider of the Yango application in the EEA. Ridetechn International B.V. acts as the data controller for most of the personal data processed in connection with the Yango application. According to the investigation, Yandex LLC is also involved in the processing of personal data in connection with the Yango application. We therefore consider that this operator should be treated as a data controller in accordance with the GDPR.

On 3 August 2023, we became aware that, on 1 September 2023, a law will enter into force in the Russian Federation which gives the Russian authorities a broad right of access to the data of taxi passengers. On the grounds set out below, we intend to suspend any transfer of personal data from Norway to the Russian Federation in the context of the Yango application before the entry into force of this law.

### **Advance notification**

Pursuant to Section 16 of the Norwegian Public Administration Act, we hereby notify Ridetech International B.V., Yandex LLC and Yango Norway AS (“you”, “your”) that we intend to make the following decision against you:

- 1. Processing of personal data in the context of the Yango application is contrary to the general principle of Article 44, Article 46 and Chapter V of the GDPR on transfers of personal data to third countries.*
- 2. The conditions for the urgency procedure under Article 66(1) of the GDPR are met.*
- 3. We hereby impose a ban on processing the personal data of users of the Yango application in order to transfer them from Norway to the Russian Federation, pursuant to Article 58(2)(f) of the General Data Protection Regulation.*

*Pursuant to Articles 58(2)(j) of the GDPR, we order you to suspend the transfer of personal data collected in connection with the Yango application from Norway to the Russian Federation.*

*The ban on processing and the order to suspend data transfers will enter into force on 1 September 2023. This is a provisional decision under Article 66(1), valid for a period of three months until 30 November 2023.*

Yango Norway AS is included as it is a Norwegian establishment of the Yandex LLC and/or Ridetech International B.V.

Please provide any comments you may have by **14 August 2023**. Comments should be sent to [Trine.Smedbold@Datatilsynet.no](mailto:Trine.Smedbold@Datatilsynet.no), [Guro.Asbo@Datatilsynet.no](mailto:Guro.Asbo@Datatilsynet.no), [Sebastian.Forbes@Datatilsynet.no](mailto:Sebastian.Forbes@Datatilsynet.no), [Tobias.Judin@Datatilsynet.no](mailto:Tobias.Judin@Datatilsynet.no) and [postkasse@Datatilsynet.no](mailto:postkasse@Datatilsynet.no).

### **Applicable law**

#### Transfers of personal data to third countries

Transfers of personal data to third countries or international organisations are laid down in Chapter V of the General Data Protection Regulation. The general principle of transfers is laid down in Article 44 of that Chapter, according to which any transfer of personal data which are

undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in that Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions of that Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 46 of the GDPR provides for transfers of personal data subject to appropriate safeguards. Pursuant to paragraph 1 of that Article, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

According to paragraph 2 of that Article, the appropriate safeguards referred to in paragraph 1 may be provided for, without requiring a specific authorisation from the supervisory authority, by: a legally binding and enforceable instrument between public authorities or public bodies; binding corporate rules pursuant to Article 47 GDPR; standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) GDPR; standard data protection clauses to be adopted by the data protection authority and adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) GDPR; adopted codes of conduct referred to in Article 40 GDPR, together with binding and enforceable commitments by the controller or processor of the third country, for the application of appropriate safeguards, including the rights of data subjects; the approved certification mechanism referred to in Article 42 GDPR, together with binding and enforceable commitments by the controller or processor of the third country, for the application of appropriate safeguards, including the rights of data subjects.

Subject to the authorisation of the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also include, in particular, the following: contractual clauses between the controller or processor and the controller, processor or recipient of the data in a third country or international organisation; or (b) provisions to be included in administrative arrangements between public authorities or public bodies and which include enforceable and effective rights of data subjects.

The supervisory authority shall apply the consistency mechanism referred to in Article 63 GDPR in the cases referred to in paragraph 3 of Article 46 GDPR. The approvals granted by a Member State or a supervisory authority pursuant to Article 26(2) of Directive 95/46/EC shall remain valid until such time as the supervisory authority concerned amends, replaces or revokes them where necessary. Decisions adopted by the Commission pursuant to Article 26(4) of Directive 95/46/EC shall remain in force until they are amended, replaced or repealed where necessary by a Commission decision adopted in accordance with paragraph 2 of this Article.

#### Powers of the supervisory authority

Article 56 of the GDPR provides for the powers of the lead supervisory authority. Article 60 of the GDPR provides for cooperation between lead supervisory authorities and the supervisory authorities concerned.

Article 58 of the GDPR sets out the powers of the supervisory authorities. In accordance with subparagraph 2(f) of that article, the authority may impose a temporary or definitive limitation on processing, including a ban on processing. In accordance with subparagraph 2(j) of that article, the authority may order the suspension of data flows to a recipient in a third country or to an international organisation.

### Urgency procedure

Article 66 of the GDPR on the urgency procedure reads as follows:

- 1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.*
- 2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.*
- 3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.*
- 4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.*

## **Our assessment**

### On the lawfulness of data transfers

A case concerning the Yango application and the lawfulness of transfers of personal data has been the subject of a cooperation procedure between the European Data Protection

Authorities. According to that investigation, the personal data relating to users of the Yango application are transferred to the Russian Federation on the basis of safeguards under Article 46 of the GDPR. These safeguard measures are, in-and-of themselves, compatible with the GDPR and, in principle, allow the transfer of personal data to a third country for which the Commission has not taken a decision on an adequate level of data protection in accordance with Article 45 of the GDPR. However, the safeguards do not create an absolute right for the controller to transfer data to a third country. The controller must also ensure that data transfers comply with the general objectives of the General Data Protection Regulation as interpreted by the Court of Justice of the European Union.<sup>1</sup> In particular, following the judgment of the Court of Justice in *Schrems II*, such an assessment must take into account whether the authorities of a third country have access to the personal data transferred.<sup>2</sup>

In practice, the Court has held that a competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country on the basis of standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority, it considers, in the light of all the circumstances of that transfer, that those clauses are not or cannot be complied with in that third country and that the protection of the data transferred, as required by EEA law, and in particular by Articles 45 and 46 of the GDPR in light of the Charter, cannot be ensured by other means, in so far as the controller established in the Union or its processor has not itself suspended or terminated the transfer.<sup>3</sup> This may be due, for example, to the legislation of the relevant third country.

The activities of the controllers have been examined in the cooperation procedure between supervisory authorities under Article 60 of the GDPR. However, the new legislation, which will enter into force on 1 September 2023, creates the right for the executive authority of the Russian Federation's security services to have 24/7 remote access to databases and information systems used to receive, store, process and dispatch taxi orders. This allows the said authority to have very wide access to personal data collected from data subjects residing in Norway.

In *Schrems II*, the Court of Justice emphasised that the exceptions and limitations on the protection of personal data (which includes the disclosure of such personal data to a public authority) must be proportionate to the objectives pursued and must apply only in so far as is strictly necessary. The legislation in question must contain clear and precise rules governing the scope and application of the exception or restriction and must lay down safeguarding measures for exceptions and limitations. In particular, the legislation must lay down conditions for the exceptions and limitations that ensure that the protection of personal data is no more limited than necessary.<sup>4</sup> Such conditions often include *ex ante* control measures restricting public authorities' access to data, such as a separate decision by an independent court on the authority's right of access. In the present case, there are no such safeguards. The

---

<sup>1</sup> Judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner vs Facebook Ireland and Maximilian Schrems ('Schrems II'), paragraphs 90 to 121

<sup>2</sup> Schrems II, paragraph 104

<sup>3</sup> Schrems II, paragraph 121

<sup>4</sup> Schrems II, point 176

national authority would have extensive and unrestricted access to the data under the legislation that enters into force in the Russian Federation.

We consider that there is a significant and concrete risk that personal data collected from Norway and transferred to the Russian Federation would be processed in a manner that does not meet the requirements of the GDPR or the data transmission mechanisms provided for therein.

#### Handling a case under the urgency procedure

A case concerning the processing of personal data that has an impact on the territory of several EEA Member States is dealt with in the so-called cooperation procedure under Article 60 GDPR. Under this procedure, the lead supervisory authority shall be determined by the main establishment of the controller as defined in Article 4(16). In the present case, the service provider of the Yango application in the EEA is, according to a previous investigation, Ridetech International B.V. (formerly Yandex.Taxi B.V.) based in the Netherlands. Consequently, the Dutch supervisory authority Autoriteit Persoonsgegevens has been assumed as the lead supervisory authority in Yango cases. The other supervisory authorities involved in Article 60 procedures shall be the supervisory authority concerned, as defined in Article 4(22). We are a supervisory authority concerned.

However, in accordance with Article 66(1) of the GDPR, and by way of the derogation that is provided for in exceptional circumstances, the supervisory authority concerned may immediately adopt provisional measures.

In connection with a telephone conversation with the journalist from Helsingin Sanomat on 3 August 2023, the Finnish Data Protection Ombudsman was informed of new legislation concerning taxi service providers that will enter into force in the Russian Federation on 1 September 2023. This information was then conveyed to us. In the Russian Federation, a federal law adopted in December 2022 requires<sup>5</sup> a taxi service provider to provide the federal security executive, or its regional body, with access to taxi service information systems and databases. With regard to the Yango taxi application, such information could include, for example, the addresses from which the customer was picked up and to which he or she was taken.

In accordance with Article 14(7) of the Act on the Organisation of the Carriage of Passengers and Baggage by Passenger Taxi in the Russian Federation, access shall be given to information systems and databases used for the receipt, storage, processing and transfer of passenger taxi orders in a manner prescribed by the Government of the Russian Federation.

---

<sup>5</sup> Law of the Russian Federation No. 580-FZ on the organisation of the carriage of passengers and baggage by passenger taxis in the Russian Federation, amending certain acts of the Russian Federation and recognising certain provisions as invalid. The law was approved in Duma on 22 December 2022, the law was approved by the Federal Council on 23 December 2022, and the President signed the Act on 29 December 2022. The law can be read from an online service maintained by the Russian authorities: [actual.pravo.gov.ru/text.html#pnum=0001202212290039](https://actual.pravo.gov.ru/text.html#pnum=0001202212290039), visited 4.8.2023

The Government of the Russian Federation adopted a decree on the same subject on 4 July 2023.<sup>6</sup> The Regulation lays down rules requiring the security executive to have access to the information of the taxi service. In accordance with paragraph 2 of the rules laid down by the Regulation, the passenger taxi subscription service operating on an online service shall provide the executive of the State Security Service with 24/7 remote access to information systems and databases used to receive, store, process and dispatch taxi orders.

The aforementioned law of the Russian Federation concerning the provision of information, as well as the Decree of the Government of the Russian Federation, which supplements it, will enter into force on 1 September 2023.

As stated above, we consider that you will not be in a position to comply with the safeguards provided for in Article 46 GDPR nor the safeguards provided elsewhere in the GDPR, in particular following the entry into force of the law on the Organisation of the Transport of Passengers and Baggage by Passenger Taxis in the Russian Federation. Since this legislation enters into force on 1 September 2023, the matter must be dealt with under the urgency procedure referred to in Article 66 of the GDPR. In particular, it would not be possible to deal with the matter under the ordinary cooperation procedure before the entry into force of that law, since the procedural provisions of Article 60 GDPR takes at least four weeks to complete.

On the basis of the above, we consider that the unrestricted access of the Russian Federation's National Security Service to the personal data of taxi passengers seriously jeopardises the fundamental rights and freedoms of data subjects in Norway. For this reason, the urgency procedure provision is also necessary in order to protect the interests of data subjects.

Given the exceptional circumstances which have arisen from the new legislation, the urgency of the matter, the lack of appropriate safeguards and the risks to the rights and interests of data subjects, we consider that the requirements for the need for exceptional circumstances and urgent measures referred to in Article 66(1) GDPR are met in this case.

### **Further consideration of the case and considerations to be taken into account**

On the basis of a clarification by the controller in April 2022, the controller's main establishment, as referred in Article 4(16) GDPR, is assumed to be located in the Netherlands. In August 2023, the Office of the Data Protection Ombudsman was informed by the Dutch supervisory authority that a number of mergers and acquisitions have taken place in the Yandex group. In view of the fact that the intended decision constitutes a temporary emergency measure to safeguard the rights and freedoms of data subjects in Norway, a further analysis of the matter may continue to be carried out as to if and how the mergers and acquisitions affect who is to be considered the controller, as regards the personal data processed in the context of the Yango application. This could also have an impact on who is to be regarded as a competent supervisory authority.

---

<sup>6</sup> Decree N. 1101 of the Government of the Russian Federation of 4 July 2023, which can be read from the online service operated by the Russian authority: <http://publication.pravo.gov.ru/document/0001202307070021>, visited 4.8.2023

A final decision may be taken by the lead supervisory authority, the EDPB or us as a competent supervisory authority.

Kind regards

Tobias Judin  
Head of International Section