Statement

Statement 02/2022 on personal data transfers to the Russian Federation

Adopted on 12 July 2022

The European Data Protection Board has adopted the following statement:

Since 24 February 2022, the Russian Federation (Russia) is in a *de facto* state of war against Ukraine. As a consequence, it was excluded from the Council of Europe on 16 March 2022. Therefore, Russia is no longer a contracting party to those conventions and protocols concluded within the framework of the Council of Europe that are open only to its member States. It will also cease to be a High Contracting Party to the European Convention on Human Rights as of 16 September 2022.

While, in its decision adopted on 23 March 2022, the Committee of Ministers of the Council of Europe stated that Russia will continue to be a contracting party to those conventions and protocols concluded in the framework of the Council of Europe to which it has expressed its consent to be bound and which are open to accession by non-member States – for instance, Convention 108 –, the modalities of Russia's participation in these instruments are still to be determined[1]. Such changes could have a significant impact on the level of protection of data subjects.

The European Data Protection Board (EDPB) recalls that the transfer of personal data to a third country, in the absence of an adequacy decision of the European Commission pursuant to Article 45 GDPR, is only possible if the controller or processor has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies are available for data subjects (Article 46 GDPR). In the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR, a transfer or a set of transfers of personal data to a third

[1] According to the Resolution CM/Res(2022)3 on legal and financial consequences of the cessation of membership of Russia in the Council of Europe, the modalities of Russia's participation in these instruments shall be determined separately for each of them by the Committee of Ministers or, when appropriate, by the State Parties.

country shall take place, in specific circumstances, only on one of the conditions set forth in Article 49 GDPR ("Derogations for specific situations")[2].

Russia does not benefit from an adequacy finding by the European Commission in accordance with Article 45 GDPR. Therefore, transfers of personal data to Russia must be carried out using one of the other transfer instruments provided for in Chapter V GDPR. Having this in mind, the EDPB notes that, when personal data are transferred to Russia, data exporters under the GDPR should assess and identify the legal basis for the transfer and the instrument to be used among those provided by Chapter V GDPR (e.g., Standard Contractual Clauses or Binding Corporate Rules), in order to ensure the application of appropriate safeguards.

Furthermore, the EDPB recalls that, following the *Schrems II* ruling of the European Court of Justice[3], and according to the EDPB Recommendations on supplementary measures[4], data exporters should assess if, in the context of the transfer at stake, there is anything in the law and/or practices in force in Russia (in particular, regarding access to personal data by the Russian public authorities, especially for criminal law enforcement and national security purposes) that may impinge on the effectiveness of the appropriate safeguards provided by the transfer instruments identified. If this is the case, data exporters should identify and adopt supplementary measures that are necessary to ensure that data subjects are afforded a level of protection that is essentially equivalent to that guaranteed within the EEA[5]. Where such assessment leads to the conclusion that compliance is not (or no longer) ensured, and that no supplementary measures could be identified, data exporters have to suspend data transfers.

Several Member States of the EEA have close economic and historic ties with Russia, therefore frequent exchanges of personal data occur between these countries and Russia. Some national data protection supervisory authorities are already looking into the lawfulness of data transfers to Russia, including in the context of ongoing investigations. Supervisory authorities will continue to monitor legislative changes and other relevant developments in Russia that could have an impact on data transfers. They will handle cases involving data transfers to Russia taking into account the increased impact on the rights and freedoms of data subjects that may arise from such data processing operations, and will coordinate within the EDPB, as appropriate.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

[2] See Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

[3] CJEU, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559.

[4] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version adopted on 18 June 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[5] The European Economic Area, abbreviated as EEA, consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway; excluding Switzerland).