Feb 2019

Russia: Harmonising data protection laws with the EU

The Council of Europe ('CoE') issued a Protocol ('the Protocol') Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') in October 2018. The signing of the Protocol by Russia may facilitate cross-border transfers of personal data between Russia and other signatories of Convention 108. Stanislav Rumyantsev, Senior Lawyer at Gorodissky & Partners, discusses the differences between Russian data protection law and that of the EU, and the amendments Russia may need to make in order to harmonise its laws with the provisions of Convention 108.

Grey_Coast_Media/Envatoelements

2018 went down in history as the year of important privacy developments. Several months after the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') had come into effect, the CoE introduced noteworthy amendments to Convention 108 through the Protocol. Russia was among the first signatories, and this may eventually facilitate cross-border transfers of personal data between Russia and other countries.

Convention 108

The CoE opened Convention 108 for signature in 1981. This is the first binding international instrument establishing global standards for protecting individuals' privacy and balancing their privacy rights with the concept of free flows of personal data across national borders. It is one of the frontrunners of the GDPR.

The CoE is an international organisation comprising 47 countries of Europe, including non-Member States such as Russia. It is sometimes confused with the Council of the European Union because of their similar names. The Council of the European Union is the main decision-making body of the EU, which enacted the GDPR (together with the European Parliament), and not an international organisation.

The Protocol

The world has changed much since Convention 108 was first adopted, so amendments were highly expected. On 10 October 2018, the first 22 countries signed the Protocol, with the aim to 'address the challenges to privacy resulting from the use of new information and communication technologies, and strengthen Convention 108's mechanism to ensure its effective implementation[1].'

The Protocol should enter into force three months following the date on which all parties to Convention 108 have given their consent to be bound by the Protocol (53 countries in total, including several non-members of the CoE, such as Uruguay). Giving such consent implies ratification, acceptance or approval, depending on national laws. If at least 38 parties join the Protocol and the remaining states fail to do so within the next five years, the Protocol should be binding only on those parties who gave their consent. As of today, the Protocol has been signed by Austria, Bulgaria, Finland, France, Germany, Iceland, Ireland, Netherlands, and Sweden, among others.

The Protocol does not copy the wording of the GDPR, but reflects similar concepts. Thus, the provisions of the Protocol were obviously formulated taking into account the basic data processing principles formulated under the GDPR (lawfulness, fairness and transparency, purpose limitation, accountability, and others). All countries signing the Protocol must harmonise their domestic laws to give effect to the amendments it introduces to Convention 108.

Cross-border data flows under the GDPR

According to Article 17 of the Protocol, the parties to Convention 108 should not prohibit or subject to special authorisation the transfer of data to a recipient who is under the jurisdiction of another party, for the sole purpose of personal data protection. Does this rule provide for the free flow of data from EU Member States to non-EU countries joining Convention 108?

This is not the case for Russia, at least in the near future. The Protocol states that a party to Convention 108 may prohibit cross-border transfers or subject them to special authorisation if this party is 'bound by harmonised rules of protection shared by states belonging to a regional international organisation.' The GDPR undoubtedly falls under this exception. Under Article 45 of the GDPR, data can be unimpededly transferred from the EU, only to countries ensuring an adequate level of protection. The adequacy level should be assessed by the the European Commission ('the Commission'). The Commission has so far recognised only 12 countries and territories as providing adequate protection, and Russia has not been shortlisted[2].

Consequently, EU-based companies must secure their data transfers into the territory of Russia with one of the appropriate safeguards specified under Article 46(2) of the GDPR. In most cases, they offer Russian subsidiaries, partners and contractors to enter into the Standard Contractual Clauses ('SCC') adopted by the Commission. If an EU company acts as a controller and its Russian counterpart as a processor, the SCC must be concluded together with a data processing agreement, in line with Article 28 of the GDPR. While some Russian companies sign on the dotted line, others get stuck with the collisions between Russian law and the GDPR. For instance, there are differences in terminology, data security measures and several other mandatory contractual provisions. In general, it seems possible for many Russian companies to comply with the SCC and the processor's obligations as per Article 28(3) of the GDPR while dealing with the EU data, but the compliance requires additional efforts and costs as compared to

those necessary under Russian law. Furthermore, the use of SCC as an adequate safeguard may be challenged by the so-called *Schrems II* case brought to the Court of Justice of the European Union[3]. These are the main reasons why both EU-based and Russian companies would benefit from facilitating data flows and the harmonisation of Russian laws with the European standards.

How Convention 108 may help with obtaining an adequacy decision

Russia's accession to the Protocol will not release businesses from establishing appropriate safeguards, but it still plays an important role from a GDPR perspective. According to Recital 105 of the GDPR, the Commission should take into account the third country's accession to Convention 108 while assessing the adequacy of the level of protection in that country. In addition, the assessment covers the existence and effective functioning of a data protection authority, the rule of law, respect for human rights and freedoms, implementation of data protection rules and security measures, enforcement of data subject rights and other elements.

Since Russia's Federal Service for Supervision of Communications, Information Technologies and Mass Communications ('Roskomnadzor') announced Russia's intention to receive an adequacy decision[4], the signing of the Protocol seems to be the first step towards substantial development of the Russian laws. Below is a brief summary of Russia's homework for implementing the Protocol.

Cross-border transfers under Russian law

In line with Article 17 of the Protocol, the Russian Federal Law of 27 July 2006 No. 152-FZ on Personal Data, (as amended) ('the Personal Data Law'), allows hassle-free transfers of data into the territory of any party to Convention 108 or any other country supporting an adequate level of data protection as recognised by Roskomnadzor. The adequacy test includes compliance of the domestic laws of such countries with the provisions of Convention 108.

The Protocol requires that Russian cross-border transfer rules be supplemented with the possibility to ensure an adequate level of protection by ad hoc or approved standardised safeguards that are (i) legally binding and enforceable; and (ii) adopted and implemented by the persons involved in the transfer and further processing. For instance, such safeguards may exist in the form of contractual clauses or binding corporate rules (same as prescribed under the GDPR).

Controllers and processors

According to the Protocol, personal data should be processed by controllers and processors. Controllers have decision-making power with respect to data processing, and the processors actually process the data on behalf of the controllers. The Personal Data Law does not use these terms. In Russia, the 'operators,' alone or jointly with others, organise the data processing and/or process the data, as well as determine the data categories to be processed, and the processing purposes and actions. Hence, almost any person or entity dealing with personal data should be treated as an operator. The operator bears most of the data protection obligations prescribed by Russian law. Under Article 6(3) of the Personal Data Law, a third party may process personal data on the instruction of the operator in the form of an agreement, or a statutory or municipal act. From a formal point of view, such a third party may be also treated as a data operator. That is why the allocation of responsibilities and roles in data processing is not as clear under Russian law as it should be, according to the Protocol.

Data subject rights

The Protocol lays down new data subject rights. Most of them already exist in Russian law, e.g. the right not to be subject to a decision significantly affecting the data subject and based solely on automated data processing, and the right to inquire about the reasoning underlying the data processing. The Protocol introduces the right to object to the processing of personal data that is new to the Personal Data Law and already addressed in greater detail under the GDPR.

Sensitive data

According to the Protocol, Russia should explicitly recognise genetic data as sensitive information and set out appropriate safeguards.

Data breach notification

Russian law should be supplemented with the controller's obligation to promptly notify at least Roskomnadzor of data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects. Under the current edition of Article 21(3) of the Personal Data Law, the operator must notify Roskomnadzor of the elimination of a data breach if such a breach was revealed and eliminated at the request of Roskomnadzor. The same rule applies to notifying the data subject if a breach was cured at their request.

Impact assessment

Article 12 of the Protocol requires that controllers and processors (where applicable) examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects beforehand. The assessment should be focused on proportionality and examination of risks[5]. This procedure refers to one of the main GDPR concepts. Article 18.1(1) of the Personal Data Law mentions such assessment as one of the compliance procedures, but it is not identical to those specified under the Protocol and the GDPR. The Personal Data Law does not establish any further regulations on this matter.

What to expect

Sooner or later, Russia will amend the Personal Data Law with a view to implementing the Protocol and harmonising it with the laws of other parties to Convention 108. International businesses have good reasons to expect that the upcoming legislative changes will unify the Russian data protection rules with those under the GDPR to some extent, and eventually facilitate data processing operations. As to the cross-border transfers, it seems unrealistic that the adequacy decision can be received by Russia anytime soon, but the tendency towards developing data privacy in Russia is positive overall. The unification may lead to simplifying compliance work in the Russian offices of international companies.

At this early stage, it is unclear how deep the harmonisation of Russian law with the laws of other Convention 108 parties could be, and when to expect the amendments. It is advisable therefore for all concerned entities to keep monitoring the Russian laws and be prepared for bringing their data processing in line with new standards.

Stanislav Rumyantsev, Senior Lawyer
rumyantsevs@gorodissky.ru
Gorodissky & Partners, Moscow

1. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223
2. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CN0311
4. https://rkn.gov.ru/news/rsoc/news62380.htm
5. Section 88 of the Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91a

RELATED CONTENT

NEWS POST

Germany: BayLDA publishes findings on website providers audit

NEWS POST

EU: EDPB issues opinion on draft administrative arrangement for data transfers

NEWS POST

Russia: Bill on data transfers and telecom cybersecurity obligations passes first reading of Duma

NEWS POST

Australia: Government introduces whistleblower bill to House of Representatives

NEWS POST

Massachusetts: Senator introduces consumer data privacy bill