Volume 14, Issue 6
cecileparkmedia.com

DATA PROTECTION LEADER

A **Cecile Park Media** publication | June 2017

The double burden: Russia and the GDPR

Anastasia Petrova of Alrud unpacks how the jurisdictional scope and legal requirements under both the GDPR and Russian data protection legislation could produce duplicitous obligations for international companies.

CPM CECILE PARK MEDIA

Anastasia Petrova Associate
apetrova@alrud.com
Alrud, Russia

The GDPR: How will it affect multinational businesses in Russia and Russian businesses abroad?

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') formally enters into effect on 25 May 2018. Although the GDPR will not have a direct effect on Russia, as a non-EU Member State, it will impact the operations of multinational business in Russia and Russian businesses abroad. Anastasia Petrova, Associate at Alrud, unpacks how the jurisdictional scope and legal requirements under both the GDPR and Russian data protection legislation could produce duplicitous obligations for international companies.

The prospect of double burdens

The GDPR applies to the entities having establishments within the EU, as well as to those that do not have physical presence in the EU where their processing activities, either as a data controller or processor, are related to the offering of goods or services to data subjects in the EU, or to the monitoring of data subjects' behaviour, taking place within the EU. Due to this, Russian e-commerce companies and other online services are becoming concerned about the application of the GDPR and potential EU sanctions, which are much higher than the sanctions for breaches of Russian privacy laws.

Consequently, it seems that many Russian subsidiaries of EU companies may face a double burden in terms of bringing their processes into compliance with both Russian data protection regulations and the GDPR. Russian companies that have EU partners, suppliers and clients will be in the same boat, as EU contractors will need to ensure contractually that their Russian partners comply with the GDPR's provisions. The GDPR imposes certain obligations on data controllers aimed at ensuring that the necessary contractual arrangements are in place when companies appoint data processors or share the data with other data controllers. Thus, the GDPR requires a review of all existing agreements with the data processors of EU companies and other data controllers processing the data received from EU companies. Taking this into account, it seems that it will be a primary goal for European and Russian lawyers to find a balance where both Russian and European businesses and regulators feel equally satisfied.

Questions of jurisdiction

Another issue that arises following the entry into effect of the GDPR is the position of the Federal Service for the Supervision of Communications, Information Technology and Mass Communications ('Roskomnadzor') and its readiness to accept foreign regulations and the scope of such acceptance. The GDPR provides for certain regulations that are not currently included in Russian privacy laws. Among these are requirements for the notification of data breaches. Companies will have to notify such data breaches to the relevant regulator within 72 hours. According to the GDPR, the regulator is the supervisory authority in the country where the controller/processor has its main establishment. Each company must define the country where the regulator relevant for its business is located. In circumstances where this question is assessed with regard to the Russian subsidiary of an EU business, it seems that this may be the regulator in the EU Member State. However, it is not clear which regulator will be authorised to deal with the businesses that have their main establishment outside the EU and are covered by the GDPR.

In addition, the GDPR is already famous for the potential fines amounting to tens of millions of Euros. Even with respect to the 'reasonability of the fines' approach, such sums seem enormous in comparison with the volume of worldwide business activities of Russian entities. The question here, especially for the entities that do not have physical establishments in the EU, is how the liability terms will apply to them and how they are going to be enforced, if applied. In addition, the matter is still: what are the consequences of a failure to comply with an order to pay a fine? Indeed, Article 58 of the GDPR provides supervisory authorities with the power to impose a temporary, or definitive limitation on an entity's activities, including a ban on processing. In comparison, the Russian Law of 27 July 2006 No. 152-FZ on Personal Data provides the Roskomnadzor with the power to restrict the access to an online resource, either a website, or an application, upon a Russian court decision. This was seen, in particular, in the case involving LinkedIn Corp., as a result of which the social networking service has been unavailable in Russia since November 2016. However, it is still unclear how enforcement is going to work in cases of breaches of the GDPR by Russian businesses, considering that the Roskomnadzor is not authorised to control compliance of Russian business with the GDPR and does not have the respective mechanisms and cooperative agreements in place with the EU.

Therefore, how should the application of the GDPR be considered, with regard to jurisdictions outside the EU, in particular, in the case of Russia? Firstly, the GDPR requires the performance of

Russian companies which have EU partners, suppliers and clients will be in the same boat, as EU contractors will need to ensure contractually that their Russian partners comply with the GDPR provisions.

data processing audits to answer such questions as where the personal data are used in the company; which personal data are used or processed; how these data are handled and what are the legal grounds for processing such data; how external and internal data flows are structured; what are the rights of data subjects, whose data are processed by the company; which security procedures are already in place, whether they are sufficient and what additional security procedures are required to be implemented. Further, the company shall elaborate and implement the policies, procedures, notices, consents and agreements that justify the processes of data processing, and ensure its Russian subsidiary has a data protection officer ('DPO') appointed and also that it carries out a local security assessment and local security documentation and registration with the Roskomnadzor.

Comparison of obligations

The GDPR's requirements do not contradict Russian data privacy regulations, although Russian regulations provide for certain specific requirements, such as having a DPO for all legal entities, and without any exemptions; obligatory registration for almost all Russian legal entities and Russian subdivisions of foreign EU legal entities; and fewer opportunities for relying on general legal grounds for processing, other than the explicit consent given by a data subject.

The GDPR introduces a number of requirements for an individual's consent to constitute the basis for personal data processing. In particular, consent must be freely given, clear, informed and revocable. An individual's silence or inactivity cannot not be regarded as freely given consent. The GDPR does not consider as a due legal basis for data processing the consent given by individuals who are in a less advantageous position in comparison to that of a data controller. Thus, consent for processing of the data incorporated in the body of the employee's employment agreement cannot be considered as freely given and revocable. As a result, data controllers must ensure that they obtain separate, freely given and informed personal data processing consent from individuals, when processing of their data is justified by the consent. This novelty in the GDPR corresponds to the Russian consent requirements already in force. Russian data privacy laws set out specific requirements regarding written data processing consent and treat it as revocable at any time, unless the data controller has another legal ground to continue data processing. This concept is aligned with the EU concept of processing in accordance with the data controller's legitimate interest or due for the performance of legal obligations or a contract with the data subject, where the data subject refused to provide the consent or revoked it.

Similarly to the GDPR, Russian data privacy laws require the audit of all data processing activities performed by the data controller as a primary step to build proper data protection systems and achieve compliance with legal requirements. The process of bringing a company's processes in compliance with the GDPR may be amalgamated with the process of bringing its Russian subsidiaries' activities in line with local data protection requirements. Such an approach will allow multinational companies to reduce their costs and build legitimate and clear systems of data protection in their Russian subsidiaries.

Conclusion

As the obligations under the GDPR and Russian data protection legislation are fairly aligned, the primary concerns with regard to the GDPR from a Russian perspective are of a jurisdictional nature. In this regard, the Higher Court of Australia's statement in the key internet jurisdiction case *Dow Jones & Co. Inc. v. Gutnick* [2002] HCA 56 is of particular relevance: 'There is nothing unique about multinational business, and it is in that that this appellant chooses to be engaged. If people wish to do business in, or indeed travel to, or live in, or utilise the infrastructure of different countries, they can hardly expect to be absolved from compliance with the laws of those countries. The fact that publication might occur everywhere does not mean that it occurs nowhere.' The world will never be the same and multinational companies will have to adapt their activities to its realities. For Russian lawyers, such a challenge undoubtedly exists, and there is no other option than to accept it.