Jan 2022

Russia: Basics of biometric data processing and protection

In 2021, deep fake technologies have become a new reality. However, every coin has two sides, and there have been a number of cases where companies have reported fraudulent activities with the use of deep fake images and voice recordings. In decades past, a prevalent issue was criminals forging signatures and documents, while today, they forge individuals' identities. Ksenia Andreeva and Dmitry Simbirtsev, from Lewis & Bockius LLP, provide insight into the status of biometric data and its governance under Russian laws on personal data.

Iaremenko / Essentials collection / istockphoto.com

Indeed, the need to protect individuals' biometrics naturally evolves from technological developments and emerging risks. There is an extensive set of regulations governing the broader aspects of biometric data processing and specific issues, such as the use of governmental biometric systems. Recently, Russian lawmakers

adopted a batch of novel regulations that are aimed at restricting the use of biometric data.

Although the reform mainly focuses on the public and financial sector, some experts construe the novel regulations as an ultimate ban on the use of biometric data, which unsurprisingly could trigger many issues for businesses.

Notion of biometric data

The Federal Law of 27 July 2006 No. 152-FZ on Personal Data (as amended) ('the Law on Personal Data') defines biometric personal data as information on an individual's biological and physiological characteristics that enables the individual's identification and is used by the controller for an individual's identification.

Therefore, according to the Law on Personal Data and recent case law, the controller shall treat information as biometric personal data only in cases where the controller uses such personal data to identify an individual (or at least has an intent to do so). In other words, to qualify the individual's personal data as biometric data, it must be processed for identification purposes. Otherwise, such data will be just 'general' personal data that is subject to the less strict rules.

Unlike the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the Law on Personal Data does not directly mention the use of special technical means which constitute elements of biometric data processing. Due to this, and for quite some time, there had been room for a broader interpretation of biometric data processing that was subject to the specific rules of the Law on Personal Data. Such broad interpretation had been reflected in guidance from the Federal Service for the Supervision of Communications, Information Technology, and Mass Media ('Roskomnadzor') which was repealed in 2021. Within the repealed guidance, the Roskomnadzor mentioned, among other examples, that pure matching of an individual's face with their image on a badge by a company's security officer constitutes processing of biometric personal data.

However, during recent public events, the Roskomnadzor's representatives unofficially articulated the position that an individual's identification that is subject to the processing of biometric personal data requires the use of special technical means.

Again, although the Law on Personal Data does not mention the use of special technical means among other constituent elements of biometric personal data processing, it would be more reasonable to consider this among such elements. The reason for such an interpretation lies within the general scope of the Law on Personal Data, which applies to automatic data processing and to so-called '*quasi-automatic*' data processing, i.e. where personal data is processed without the use of automatic means but such personal data, is

contained in systematised records, and can be searched and/or accessed with the use of specific algorithm (that is unlikely possible when it comes to an individual's identification on basis of physiological or psychological characteristics).

In sum, as per the Law on Personal Data, a data controller must treat information as biometric personal data if the below conditions are met:

- the information relates to an individual's physiological or psychological characteristics;
- the controller uses such information for an individual's identification; and
- the controller uses special technical means to identify an individual using their physiological or psychological characteristics.

Legal bases for the processing of biometric data

The Law on Personal Data lays down specific legal bases for the processing of biometric data. Although it mentions an extensive set of such legal bases, in simple terms, a controller can process the biometric personal data if it has an individual's written consent for such processing, or the controller is required to process such data in accordance with Russian public laws.

Practically speaking, when it comes to general business operations in the private sector, in most cases, consent remains the only available legal basis. Alternative legal bases are very narrow and therefore apply very rarely.

The Law on Personal Data lays down very strict requirements on the form and contents of such written consent. Namely, it shall contain a set of specific elements, such as the data subject's name, address, and passport details, the controller's name and address, the processing purpose, the personal data to be processed on a basis of consent, and the processors' details, among others.

As regards its form, an individual must sign their consent in hard copy with a blue-ink signature. It is also legitimate to execute consent electronically with the use of a digital signature compliant with the specific Russian laws. Therefore, just a tick-box or a simple declaration of consent will not be a sufficient justification of biometric data processing.

Individuals may revoke consent at any moment, and the controller shall terminate consent-based processing within 30 calendar days following the consent revocation. In practice, it means that the controller should have in place a procedure to handle the revocation requests (and any other data subjects' rights requests) in a timely manner.

Protection of biometric personal data

The Law on Personal Data requires that the controller preserves confidentiality and ensures the security of personal data that it processes. To comply with this basic principle, the controller must implement a set of legal, organisational, and technical security measures.

The secondary legislation adopted in accordance with the Law on Personal Data explains how controllers must choose the appropriate security measures.

In principle these regulations introduce four levels of personal data protection and a set of basic security measures that the controller must implement to ensure the corresponding level of data protection. Level 1 is the highest and Level 4 is the lowest. The higher the required level of data protection, the more complex measures the controller should implement. However, the majority of measures prescribed by such regulations are still rather broad, which in practice enables the controllers to be quite flexible when building their data security strategies.

The required level of personal data protection depends on three basic factors, namely:

- the type of data security threats;
- the amount of data subjects concerned by the personal data processing; and
- the type of personal data processed by the controller.

Biometric data is quite sensitive in terms of its impact on individuals' privacy, which is why the processing of biometric data triggers the change to the data protection level that the controller shall implement. In case the controller processes biometric data, the lowest possible security level is Level 3, which can be raised depending on two other factors.

For example, where the controller is required to ensure Level 3 (the basic level if processing biometric data), such controller is required to appoint an officer responsible for the security of personal data, while in the case of Level 4 (lowest level) appointment of such officer is not strictly required.

Conclusion

Technologies driven by the processing of biometric data are continually evolving, but such data and the implications of its processing remain very sensitive in terms of individuals' privacy. Considering this, Russian laws lay down straightforward requirements that govern the protection and processing of biometric personal data. Data controllers conducting business in Russia should always consider the corresponding rules before they launch any processes and products that imply the processing of biometric data.

Ksenia Andreeva Partner
ksenia.andreeva@morganlewis.com
Dmitry Simbirtsev Associate

dmitry.simbirtsev@morganlewis.com
Morgan, Lewis & Bockius LLP, Moscow