Payet Rey Cauvi Pérez

CONTACT:

Carlos Patrón
Partner
cap@prcp.com.pe

Giancarlo Baella
Principal Associate
gbp@prcp.com.pe

Ana Lucía Figueroa
Associate
afd@prcp.com.pe

Marianna Vallvé
Associate
mvg@prcp.com.pe

Fernando Salhuana
Associate
fsq@prcp.com.pe

Luciana Márquez
Associate
lma@prcp.com.pe

Av. Víctor Andrés Belaúnde 147
Edificio Real 3, Piso 12 - San Isidro, L27,
Lima - Perú
prcp.com.pe

DRAFT MODIFYING THE PERSONAL DATA REGULATION IS PUBLISHED FOR PUBLIC COMMENTS IN PERU

The National Authority for the Protection of Personal Data (or "ANPDP" in Spanish), an organism within the Ministry of Justice and Human Rights, published a draft which addresses several modifications to the current Regulation of Law No. 29733, Personal Data Protection Law ("Draft Regulation").[1]

According to the ANPDP, the proposal is necessary since it would improve the current regulatory standards enacted in 2013 and update it to current trends such as "*digital technologies, e-commerce, artificial intelligence, personal data profiling, among others.*"

According to the Explanatory Memorandum of the Draft Regulation, the proposed changes reflects the recommendations by the Organization for Economic Cooperation and Development (OECD) would have provided in personal data for member countries, being that Peru would be in the evaluation phase for its accession. Likewise, the Explanatory Memorandum of the Draft Regulation highlights that the proposed changes refer to comparative regulations, particularly, the European Union's General Data Protection Regulation (GDPR), as far as they could be applied to our legislation.

In summary, the main changes to the Draft Regulation are as follows:

- **New definitions (Article II):** including, among them, terms such as "profiling", "personal data security incident", and "Personal Data Officer".[2]

- **New exceptions to the scope of application (Article IV):** In addition to the already existing exceptions, the following information will be outside of the scope of the data protection law: (i) personal data of representatives of legal entities, and (ii) data of deceased individuals.

- **Expansion of territorial scope (Article V):** the personal data regulation would apply to: (i) activities related to the offer of goods/services to Peruvian consumers even though such offer comes from abroad; and (ii) activities linked to behavioral analysis and/or profiling based on behaviors, habits, and preferences of individuals located in Peru, even though the data processing takes place abroad.

---

[1] Ministerial Resolution No. 270-2023-JUS published in the Official Gazette "El Peruano" on August 26, 2023.

[2] Profiling: An automated processing of personal data that allows a specific and continuous evaluation of personal aspects of an individual (i.e., preferences).
Personal data security incident: Breach of security that results in the unauthorized alteration, destruction, loss, or communication/exposure of personal data.
Personal Data Officer: Individual appointed by the data controller who oversees the implementation and supervision of the Personal Data Law and its Regulation.

Payet Rey Cauvi Pérez

- **Brand-New Principles (Article VII):** The "Principle of Transparency" reinforces the duty to inform the data subjects about the potential risks associated to the processing of their data and their legal rights; and the "Principle of Proactive Responsibility" states that the data controller should implement the required security measures to comply with the Data Protection Law and its Regulation and be able to show proof of documentation regarding such implementation.

- **Processing of minors' data (Articles 22 and 25):** For the processing of a minor's data, it will be sufficient to have the consent of one of the holders of parental authority or guardians, as appropriate. On the other hand, when the data processing of minors is carried out through the Internet, for the publication or dissemination of the personal data of minors over 14 and under 18 years of age through social networks (or equivalent services), the consent of the minor or, alternatively, the consent of one of the holders of parental authority or guardians, must be obtained.

- **Notification to the Authority in case of data breach incidents (Article 35):** Any incident must be reported before the ANPDP within 48 hours of its identification. Under specific circumstances, the incident must be communicated to the data subjects as well (e.g., if their rights are endangered due to the breach).

- **Personal Data Officer (Article 38):** The appointment of such official within an organization would be mandatory depending on the quantity or quality of the data processing (e.g., if it is conducted on a large-scale basis or if controller's main activity involves the processing of sensitive data). Conglomerates must appoint a Personal Data Officer, who can oversee the processing of data of the whole economic group, and it is not mandatory to appoint an officer for each company. In all cases, the officer's identity must be communicated to the public, and to the ANPDP.

- **Impact Assessment regarding the processing of personal data (Article 40):** The evaluation of the outcomes and risks of the data processing may be conducted prior to its execution. The materiality of this evaluation will increase when sensitive data is processed, personal profiles are created, or large volumes of data are processed, among other circumstances, as ruled by the ANPDP.

- **Right to data portability (Article 69):** This new right is introduced as part of the right of access established by Law. Data subjects could request from the data controller their own data on a commonly used, structured, and machine-readable format and, if deemed convenient, the transfer of the data to another controller.

- **Databanks fillings before the ANDPD (Article 89):** The registration, modification, and cancellation proceedings of data banks should be filed at no cost (i.e, free).

- **New categories of infractions (Article 140-142):** With the inclusion of new obligations in the Draft Regulation, there are now additional classifications of infractions, categorized as minor, serious, and very serious violations.[3] For example, it is considered a serious violation when "*failing to communicate to the Authority (...) the security incident when it generates exposure of personal data and/or sensitive data or when there is a high risk to the rights and freedoms of individuals*".

Finally, the phase for public comments to the Draft Regulation launched by the ANPDP will close at the end of September 2023. Please review our comments (in Spanish) through the following **link**.

[3] It should be noted that the scale of fines has not changed, that is, the maximum fine continues to be 100 Peruvian Tax Units (USD 135,000,00 approximately).

Av. Víctor Andrés Belaúnde 147
Edificio Real 3, Piso 12 - San Isidro, L27,
Lima - Perú
prcp.com.pe