

● INSIGHT

Peru: Personal Data Protection - the new Law's regulation

April 23, 2025



Summary

Peru's new Personal Data Protection regulation, enacted through Supreme Decree No. 016-2024-JUS, modernizes the legal framework to address technological advancements and strengthen privacy rights. Key changes include mandatory appointment of a Data Protection Officer, enhanced security measures, and new rights for data subjects such as data portability and protections against automated decision-making. The regulation also introduces stricter requirements for cross-border data transfers and emphasizes transparency and accountability. Organizations must adapt their policies and technologies to comply with the new standards, which aim to balance technological innovation with fundamental rights.

Peru's new data protection regulation modernizes legal frameworks to address technological advancements and strengthen privacy rights.

The protection of personal data has become a cornerstone of privacy rights in today's interconnected world. As digital technologies continue to revolutionize the way personal information is collected, processed, and shared, nations around the globe are taking steps to modernize their legal frameworks to address these new realities. In Peru, the right to personal data protection was first enshrined in the Constitution and further codified in 2011 with the

enactment of Law No. 29733, the Personal Data Protection Law. This legislation marked a pivotal moment in the country's legal history, as it sought to ensure that public and private entities handled individuals' data lawfully, transparently, and securely.

However, the rapid pace of technological advancement in recent years has exposed limitations in the original framework. Technologies like artificial intelligence (AI), cloud computing, big data analytics, the Internet of Things (IoT), and the widespread use of social media and e-commerce have dramatically altered the data landscape. Personal data is now used not only for traditional purposes but also for highly complex activities such as predictive analytics, profiling, and targeted advertising. This has raised serious concerns about privacy risks, data security, and the adequacy of existing protections.

In response to these challenges, the Peruvian Government undertook a thorough review of its data protection laws and regulations. The result of this process was the publication of Supreme Decree No. 016-2024-JUS on November 30, 2024. This regulation represents a significant overhaul of its predecessor, Supreme Decree No. 003-2013-JUS, addressing technological advancements and strengthening privacy rights for Peruvian citizens. The new provisions aim to modernize the regulatory framework, enhance compliance, and ensure Peru remains aligned with global best practices. Organizations had until March 30, 2025, to implement the necessary changes.

In this Insight article, Anita de la Piedra and David Vásquez, from Niubox Legal, discuss some key changes introduced by the regulation, including challenges and opportunities.

Key changes introduced

Strengthening data protection governance

One of the defining features of the new regulation is the emphasis on enhancing governance mechanisms for personal data protection. Central to this reform is the mandatory appointment of a data protection officer (DPO)

for organizations that process large volumes of personal data or handle sensitive data. This role is pivotal in ensuring that organizations remain compliant with the law and adopt best practices in managing privacy risks. The DPO is required to be an expert and is tasked with multiple responsibilities, including overseeing compliance efforts. Additionally, the DPO acts as the primary point of contact between the organization and the National Authority for the Protection of Personal Data (ANPD), ensuring seamless communication and transparency. By formalizing this role, the regulation emphasizes that data protection is not merely a legal obligation but a critical organizational priority.

Another key provision in the updated regulation is the requirement for foreign entities that process personal data belonging to Peruvian citizens to appoint a local representative in or for Peru. This measure ensures that companies operating across borders are held accountable under Peruvian law, particularly when they target Peruvian individuals through goods, services, or behavioral analysis. For example, a global tech firm collecting data from Peruvian users for targeted advertising would now need to designate a representative within or for Peru to manage compliance and facilitate communication with regulatory authorities.

In that line, the new regulation also introduces specific principles such as transparency and accountability. The principle of transparency implies that the processing of personal data must be informed in a clear and accessible manner to the data subject. The principle of proactive responsibility obliges organizations to implement measures to guarantee compliance with the regulations and to demonstrate said compliance.

Enhanced security and risk management

The new regulation places a stronger emphasis on proactive security measures and risk management strategies, reflecting a more comprehensive approach to safeguarding personal data. Organizations are now required to adopt the Principle of Proactive Responsibility ('Responsabilidad Proactiva'). This is a shift from reactive to proactive compliance and underscores the importance of embedding privacy into every aspect of organizational processes.

One of the most impactful updates is the requirement for mandatory breach notifications. Under the new rules, organizations must notify the ANPD within

48 hours of discovering a significant security breach. This quick response time is critical in mitigating the potential harm caused by data breaches. Organizations are also required to implement comprehensive security policies. These policies must ensure traceability in data processing, enabling organizations to track who accessed data, when, and for what purpose. This level of accountability not only reduces the likelihood of unauthorized access but also strengthens public trust in organizations' handling of personal information.

To further bolster security practices, the regulation encourages the use of Privacy Impact Assessments (PIAs). These assessments provide a structured way for organizations to evaluate risks associated with high-risk data processing activities, such as handling biometric data or processing data for AI-based profiling. By identifying vulnerabilities early, organizations can implement mitigation strategies, such as adopting more stringent access controls or anonymizing data where feasible.

Empowering data subjects

Among the novelties brought about by the new regulation were tools to empower data subjects, providing them with more security and predictability with respect to the processing of their personal data. In particular, in this section we will comment on three new provisions that have materialized in new articles of the regulation:

- reinforcement of consent requirements for marketing and commercial purposes;
- introduction of the right to data portability, enabling individuals to access their information in a usable format; and
- protections against automated decision-making without human oversight in critical situations.

Regarding the first point, with the entry into force of the new regulation of the Personal Data Protection Law, a specific article has been developed for the processing of data for advertising and commercial prospecting, which allows obtaining consent for the processing of data through a first contact. It also establishes that if consent has not been obtained, it is no longer lawful to make a new 'first' contact. In accordance with previous opinions, the article of the new regulation establishes that in order to carry out this first contact, the

personal data may have been obtained from sources accessible to the public, so the data controller must inform, in said first contact, the source of collection of the personal data if requested by the personal data subject. Secondly, another of the most important new features of the new regulation is the introduction of the right to data portability, whereas the previous regulation only regulated access, rectification, cancellation, and opposition (ARCO) rights.

This new regulation of the law introduces the right of portability as an expression of the right of access, which allows the data subject to request their data in a structured, commonly used, and machine-readable format, in order to transmit it to another data controller or personal data bank owner when the processing:

- is based on consent or on a contractual relationship; or
- is carried out by automated means.

As a third point, an important change introduced by this new regulation was the provision that established that the processing of personal data by outsourced technological means - without human intervention - may be carried out provided that it complies with the legal and regulatory provisions. As we can appreciate, the new regulation provides a higher level of protection to the holder of personal data, limiting automated decisions that may have a significant impact on the rights of the holders.

For this reason, the aforementioned article focuses on guaranteeing the right to objective processing of personal data without the intervention of the data subject, clarifying that the data controller must inform them as soon as possible about the eventual automated processing. In this sense, it introduces an explicit protection to the data subject, granting them the right not to be subject to automated decisions that produce legal effects, discrimination, or a significant impact on their life. Likewise, the data subject has the right not to be subject to automated decisions aimed at evaluating, analyzing, or predicting, without human intervention, aspects such as professional performance, economic situation, health status, and reliability or behavior.

This issue is fundamental to achieving a balance between the promotion of technological innovation and the protection of fundamental rights. Regulating automated decisions and ensuring objective treatment allows technological advances to be inclusive, ethical, and respectful of human dignity, avoiding

bias or discrimination that may arise from poorly designed algorithms or poorly managed data.

In summary, we can see that the new regulation provides the owner with new rights that empower them and promote the proper processing of their data. This not only empowers citizens but also forces organizations to adopt more accountable and transparent practices. By ensuring fair and appropriate processing, a balance is sought between the use of data and respect for fundamental rights.

Cross-border data transfers

In the previous regulation, international data transfers were possible as long as the recipient or importer assumed the same obligations as the owner of the database or data controller in Peru. However, there was no explicit mention of an assessment process to determine whether a country has an adequate level of data protection.

Now, with this new regulation, it is no longer based on the evaluation of the receiver or importer regarding compliance with the standards, but what is evaluated first is the receiving country. In this way, cross-border flow is allowed if the receiving country has an adequate level of protection that must be equivalent to that established in Peruvian law. If the country does not meet this standard, the exporter must guarantee that the data will be adequately treated, unless a specific exception of the law applies.

The assessment made by the authority to determine an adequate level of personal data protection takes into account the following elements:

- existence of a legal framework on personal data protection;
- existence of principles for data processing;
- rules that recognize and guarantee the rights of data subjects;
- the existence of an authority in charge of ensuring compliance with the rules; and
- the resolution of the Directorate is issued *ex officio* or at the request of a party.

So, while this regulation has brought more predictability with respect to the cross-border flow of personal data, there are still important challenges to consider, taking into account that the cross-border flow of data is a strategic

opportunity for Peru's economic development, provided that it is balanced with adequate protection of data subjects' rights. Ensuring this balance between economic development and the protection of data subjects' rights is key for Peru to take full advantage of the opportunities provided by the global digital economy.

Implementation timeline

The new regulation for personal data entered into force 120 calendar days after the day following its publication in the Official Gazette, El Peruano, on March 30, 2025. Some layouts had a progressive implementation. In that regard, companies had a period of four months to carry out the necessary actions to comply with the new stipulations or adapt their processes before the regulation came into effect. Therefore, it was important for companies to stay informed about the deadlines established by this regulation to avoid any breach.

In the case of data portability, which is a new right, the deadline to implement the requirements will be six months after the entry into force of this regulation. The layout for the owner of the personal data bank, data controller, or data processor related to the designation of the Personal Data Officer (PDO) has a progressive implementation schedule based on annual sales, whether it is a large, medium, small, or micro company, with a term of one to four years.

Challenges and opportunities

For companies, a huge challenge with the arrival of the new regulation is the adjustment they have to make to their internal policies and the adaptation of their contracts to the new legal requirements. As a first important point, they must carry out a detailed review to ensure that their privacy and data protection policies are clear, transparent, and accessible to data subjects. It is

vital for them to review their contracts with suppliers and third parties, the specific clauses covering the processing of personal data, as well as the security measures to be implemented. This review process is an opportunity to optimize their internal flows and implement best practices for privacy management, which can result in greater operational efficiency and minimize legal risks.

To be in order with the new standard, organizations must adopt technologies that guarantee the security of personal data; it is essential that the technological solutions adopted are robust against cyberattacks and that the integrity of the data is ensured against unauthorized access. Investing in these technologies is not only a way to comply with the law, but also an opportunity to improve the competitiveness of organizations, offer more personalized services, and foster a more direct and reliable interaction with users.

One of the greatest benefits of properly implementing the new data protection regulations is the strengthening of public trust. In a world where consumers are increasingly aware of the risks associated with the handling of their personal data, organizations that demonstrate a genuine commitment to privacy protection will be better positioned to build customer loyalty and differentiate themselves from the competition. Trust is also enhanced through ongoing communication with users about their rights and how their data is protected.

Conclusion

In conclusion, the implementation of the new regulation of the Personal Data Protection Law in Peru by the authorities represents a substantial step towards the consolidation of a robust and updated regulatory framework, with the capacity to respond to the challenges of the new digital era. This regulation not only reinforces privacy and security guarantees for individuals, but also establishes an indispensable balance between technological innovation and the preservation of fundamental rights.

Anita de la Piedra Head of Legal Solutions

adelapiedra@niubox.legal

David Vásquez Coordinator of Legal Solutions

dvasquez@niubox.legal

Niubox Legal, Peru

Topics:

Privacy Overview

Jurisdictions:

Peru

Related

GUIDANCE NOTE April 30, 2024

Peru - Employment

GUIDANCE NOTE April 9, 2024

Peru - Data Protection Overview

INSIGHT February 20, 2024

Peru: Draft Of The New Data Protection Regulation

In this Insight article, Crosby Buleje, Associate at Baker &...