Digital Compliance 2026:

Conflicts Among the Digital Code, Artificial Intelligence, and Personal Data Laws in Kazakhstan

Saule Akhmetova

Partner,
GRATA International
Kazakhstan, Almaty

2026

Digital Compliance 2026: Conflicts Among the Digital Code, Artificial Intelligence, and Personal Data Laws in Kazakhstan

In recent months, Kazakhstan's digital legislation has undergone a comprehensive overhaul. The January enactment of the Law of the Republic of Kazakhstan 'On Artificial Intelligence' (the 'AI Law'), amendments to the Law of the Republic of Kazakhstan 'On Personal Data and Its Protection' (the 'Personal Data Law'), and the extensive codification of the sector through the Digital Code of the Republic of Kazakhstan have fundamentally changed the regulatory landscape.

An analysis of the new regulatory framework has revealed systemic inconsistencies in certain provisions. In attempting to address a wide array of issues, legislators have created several 'grey areas' in legal regulation. Below are some of the legal provisions that may pose risks to businesses.

1. Recommender Systems: Classification Issues and the Autonomy Trap

An analysis of the new legislation's provisions has identified a methodological gap that poses a risk to content and commerce platforms, including marketplaces, online stores, and media outlets. The issue arises from the implementation of the AI Law regarding the classification of algorithms.

Platform owners may categorise their recommendation feeds—such as smart product suggestions or news selections—as low-autonomy systems, as outlined in Article 17.2 of the AI Law. Businesses might interpret this classification to mean that the algorithm only generates recommendations, while the final action—such as clicking on a card or making a purchase—always rests with the

end user. Following this reasoning, companies believe they are in a safe position. After all, the strict prohibitions outlined in Article 17.3 of the AI Law (including bans on hidden profiling and subconscious manipulation) are primarily aimed at high-autonomy systems.

This approach, however, contains a fundamental legal error. By defining low-autonomy systems as those in which 'a human always performs the final choice and actions', the legislator relies on the international concept of control known as *human-in-the-loop*. In this context, the 'human' refers not to the end user reacting to advertising, but rather to an operator associated with the owner of the AI system.

The recommendation algorithm's role is not to make purchases, but to select and display products algorithmically. Since the marketplace's smart feed is generated and presented to users in real time, within milliseconds, no employee can pre-check or approve each display. This means the system operates and makes decisions autonomously.

As a result of this legal ambiguity, the regulator (the Ministry of AI and Digital Development of the Republic of Kazakhstan) may reclassify a recommendation system that businesses consider harmless as having medium or high autonomy. If this occurs, the strict provisions of the AI Law will apply to standard personalised product recommendations. Moreover, any algorithm that attempts to keep a user's attention by subtly adjusting its behaviour to exploit their vulnerabilities may be categorised not as 'effective marketing', but as illegal manipulation that takes advantage of consumer weaknesses.

To avoid liability for misclassifying systems, businesses need to rethink the architecture of their recommendation services. If a company cannot ensure manual oversight of every AI action, it must implement preventative interface restrictions. Users should have a clear, technical option to completely turn off behavioural (autonomous) personalisation with a single click, switching their feed to a straightforward chronological display. This will serve as the main argument: the platform does not engage in autonomous, manipulative practices towards users.

2. Digital Marketing and Medium Autonomy: The Paradox of Instant Decisions and the Unenforceable Right to Information

Another methodological impasse arises in automated online advertising. Intelligent marketing platforms fall under the category of systems with medium autonomy (Article 17.2 of the AI Law). Unlike the illusion of 'low autonomy', here, business and the law recognise the obvious: the algorithm makes micro-decisions instantly and independently about which user to show an ad to. At the same time, the system remains within the legal framework of medium autonomy only because a human operator (marketer) exercises high-level control—they set the budget, targeting boundaries, and can cancel the entire advertising campaign at any time.

However, having successfully qualified their systems and avoided absolute prohibitions on high autonomy (Article 17.3 of the AI Law), marketers find themselves caught in the grip of another norm—the fundamental principle of transparency and explainability for all AI systems (Article 7 of the AI Law), which stipulates the user's right to information about the characteristics and limitations of the AI system, the automated processing procedures, and its consequences.

Compliance risk and a regulatory gap lurk at the intersection of technology and this general legal principle, revealing the paradox of instant automation. Deploying targeted advertising is a process in which AI makes decisions in milliseconds (to single out a specific consumer from thousands and show them a banner), leading to consequences (a change in their consumer behaviour). It is physically impossible to immediately provide a person with full information about the logic behind their profile processing and the consequences of displaying the banner, as imperatively required by Article 7 of the AI Law. Because the law fails to detail regulations for this issue across various AI systems, an insurmountable impasse arises: the technology is incapable of meeting the general requirement of real-time transparency. A post-factum regulatory review could find that the lack of immediate disclosure of the banner display logic constitutes a violation of user rights. Under the general provisions of Article 7 of the AI Law, digital marketing in Kazakhstan is moving into a compliance risk zone.

To protect businesses from legal violations arising from overly fast, automated online advertising, companies must be proactive by translating abstract legal rules into interface solutions. First and foremost, it's best to avoid working with third-party AI services ('black boxes') if their developers can't clearly explain the logic behind their targeting algorithms. Instead of complex, multi-page legal documents, it's recommended to implement a simple, clear welcome screen on a website or mobile app. It should clearly and concisely disclose the AI's operating principles to the user in advance, explaining that the system will analyse their browsing activity solely for personalised offers. When the user sees such a warning and consciously consents before algorithmic processing begins, the law's otherwise unfeasible transparency requirement becomes a clear contract between the company and its client.

3. Regulatory Barrier: Extracting Open Data at the Intersection of Business and Anti-Spam

Unlike previous legislative provisions, the legislator has left no 'grey areas' for businesses regarding the collection of publicly available personal data. Article 7.11 of the Personal Data Law formulates an uncompromising, direct prohibition: the collection and processing of personal data for the creation or expansion of any databases through unauthorised extraction from publicly available sources is strictly prohibited. This provision imposes a strict regulatory barrier to compiling commercial lists from the internet. Moreover, the law makes no distinction between high-tech and manual labour: any method of extracting information—from automated parsing to the simple manual copying of contacts—is prohibited. The scope of this prohibition is revealed by the complex dual nature of law enforcement, affecting both the business environment and the everyday lives of citizens.

On the one hand, in the area of purely business communications, the regulator may apply a flexible, limited interpretation of the right to privacy. When a lawyer, notary, or independent consultant publicly publishes their full name and work phone number on an official website, the information is purely professional. The assessment of such information by the authorised body may be biased toward a 'business context', since publishing contact details here is a condition of practising law. However, even in this segment, collecting contacts

for inclusion in third-party commercial CRM systems (whether by a marketing bot or a sales manager) is now formally recognised as non-targeted and illegal unless consent has been obtained.

On the other hand, the true purpose of the legislative barrier is to protect ordinary citizens from aggressive B2C marketing. Open digital platforms, telephone directories, and bulletin boards have served as free sources for businesses for years. The mass collection of numbers and email addresses from ordinary individuals has led to an increase in intrusive spam. The new regulation has eliminated the illusion of 'nobody's data online', declaring that the fact that a person has posted their phone number or email address online (for example, to sell a piece of furniture) does not give a third-party company the right to collect this number for subsequent calls and electronic communications. Any accumulation of such information without the data subject's express and targeted consent is now a violation, subject to sanctions.

To protect a company from regulatory scrutiny, businesses must completely phase out the practice of collecting contacts from external public sources, ceasing both automated scraping and employee-created manual database creation. The only legal way to build a customer base is through inbound marketing, where potential clients and partners voluntarily and knowingly submit their information. In practice, this requires transferring communications to the organisation's own resources, such as corporate websites, landing pages, or secure subscription forms. In this model, the user, by filling out a form or registering for a webinar, performs the target action on the screen, thereby granting the company the legal right to process their data, eliminating the risk of accusations of inappropriate extraction of information from publicly available sources.

4. Digital Architecture Crisis: The Systemic Trap of Undefined Identifiers for Corporate IT

The new rules have created a problem that extends far beyond online marketing and affects virtually all digital business systems—from retail loyalty systems to internal ERP, CRM, and HR platforms. This situation arose due to inconsistent regulations. On the one hand, Article 45 of the Digital Code

introduces the category of digital data identifiers, defining unique identifiers for individuals and legal entities. On the other hand, the Personal Data Law has changed the definition: personal data now means information about an individual supplemented by one or more *identifiers*. As a result, this overlapping of regulations turns routine company technical processes into a zone of strict legal regulation.

The main methodological flaw and systemic legislative trap is that the Personal Data Law and the Digital Code do not specify whether the type of identifier is relevant for 'enabling' legal protection, nor do they provide even an approximate list of such digital markers. As a result, any internal digital trace could, in theory, fall under the Law's scope: a discount card number, an internal User ID in a database, a mobile app token, an employee's personnel number in an HR system, or a tracker ID on a logistics vehicle.

In theory, the combined application of these regulations poses a hypothetical risk that even the most routine digital traces could be subject to surveillance—for example, a purchase record, a building entry log, or a work time record if they are linked to an internal ID. However, it would be premature to assert this categorically. The Ministry of AI and Digital Development of the Republic of Kazakhstan could take a completely different interpretation. Based on the historical practice of the domestic regulator, the authorised body has always taken a narrow approach to interpreting personal data, considering personal information to be personal only if, in isolation, it allows the identification of an individual. For example, in one of its clarifications, it noted that an Individual Identification Number (IIN) alone, 'in isolation' from a full name, does not constitute personal data. However, the lack of clear criteria for 'complementarity' in the new definition of 'personal data', as well as the absence of a list of private identifiers in Article 45 of the Digital Code, creates predictable uncertainty for the corporate sector. No one can guarantee exactly where the authorised body will draw the line between technical log analysis and protected privacy during future audits.

To minimise risks amid this methodological ambiguity, companies must act proactively and protect their technological processes. A logical solution is to separate intelligently and structure information flows at the database architecture

level. In practice, this means that an organisation's internal IT infrastructure must be clearly segmented: technical records, log files, and private identifiers of automation systems must be processed separately from substantive, personal data about clients or employees. Any merging or 'complementation' of these data, resulting in a technical log being firmly linked to a real-life individual's profile, must be transparent and legally justified in accordance with the company's internal policies. This balanced approach will help protect businesses from unpredictable changes in regulators' interpretations of legislation.

Conclusion: From Paper-Based Compliance to Architectural Compliance

In summary, the 2026 digital legislation blurs the line between legal and IT departments. As an analysis of the hidden conflicts between the Digital Code, the AI Law, and the updated personal data regulations shows, traditional 'paper-based' compliance is ineffective. Vague wording and the rigidity of the new requirements render algorithms, marketing tools, and internal databases high-risk areas. Under these conditions, passively awaiting the first precedents and audits becomes a dangerous strategy. To successfully navigate Kazakhstan's new regulatory reality, companies must transition to a proactive compliance approach—embedding transparency principles directly into the code of algorithms (*AI-by-Design*), modifying user interfaces, and building data architectures that account for various interpretations of the law.

Saule Akhmetova

Partner,
GRATA International Kazakhstan, Almaty

sakhmetova@gratanet.com