Llinks Client Alert — December 2024 (Year-End Special Edition) What Data Compliance Tasks Are Left for 2025?

On this day that you receive this Client Alert, 2024 is coming to a close. For those specialized in the cybersecurity and data compliance, 2024 has been an eventful year. This year, in January, the *Regulations on the Protection of Minors in Cyberspace* officially came into effect, becoming the first comprehensive regulation in the field of minor's online protection. In March, the *Regulations on the Promotion and Standardization of Cross-Border Data Flow* eased the cross-border data compliance obligations for most enterprises. In April, the Ministry of Industry and Information Technology ("**MIIT**") issued an announcement to launch the pilot program for the expansion of value-added telecommunications services to open up to foreign markets. In May, the *EU Artificial Intelligence Act* was passed, providing important insights for China's AI regulation and governance. In the same month, free trade zones such as Shanghai and Tianjin released positive and negative lists for cross-border data transfer, providing new compliance pathways for data transfer. In July, the draft national standard *Personal Information Protection Compliance Audit Requirements* heated up discussions on personal information compliance audits. In September, the *Regulations on Network Data Security Management* were released, reaffirming and elaborating on several key data compliance obligations. Most recently, in December, the *Regulations on Data Security Management for Banking and Insurance Institutions* were formally issued, setting the tone for financial institutions' data compliance objectives.

In terms of law enforcement, we observed the following trends for 2024: Regulation of mobile applications and other internet products is becoming routine. For instance, MIIT regularly tests APPs (SDKs) and publicly discloses violations. Globally, the security of cross-border data transfers is increasingly under scrutiny. In July, a Chinese entity was fined 20 billion KRW for violating Korean cross-border data transfer regulations. The number of penalties in the data security field has significantly increased, and the "dual investigation" model has become common. This means that when handling data security incidents, both the attacker's responsibility and the accountability of relevant companies for failing to fulfill data security protection obligations are being pursued. The governance of algorithms has also become a major regulatory focus. In November, the Cyberspace Administration of China ("**CAC**") and three other departments jointly launched the "Clear and Bright · Governance of Typical Problems in Network Platform Algorithms" initiative, aiming to solve the problem of algorithm abuse and protect user rights.

Legislative and law enforcement activities in the cybersecurity and data compliance fields have been fast-paced, keeping data compliance professionals constantly on their toes and sometimes struggling to keep up with new compliance obligations. As we move into 2025, what new compliance obligations need to be met, and which existing ones need to be reinforced? The Llinks Cybersecurity and Data Compliance Team hereby presents an outlook for cybersecurity and data compliance work in 2025.

1. Regulatory Focus on "Internal" Aspects of Data Compliance

It has been more than three years since the *Personal Information Protection Law* ("**PIPL**") came into effect, and related enforcement activities have become routine. However, our observation shows that, in the past few years, both regulators and companies have mainly focused on the "external" aspects of personal information compliance. For example, many companies have improved their privacy policies for websites and apps and rectified personal information-related functionalities according to the PIPL, while regulators have concentrated their enforcement efforts on this area as well. For instance, since the beginning of this year, MIIT has issued 10 batches of public notifications regarding apps (SDKs) violating user rights.

However, data compliance also entails numerous equally important "internal" requirements. With the accumulation of enforcement experience by the CAC and other industry regulators in recent years, enforcement agencies have expanded their focus beyond the externally visible aspects. In the past three years, enforcement actions concerning internal data compliance obligations have risen by the year. Violations targeted by enforcement include: failure to implement data security protection technologies, unscanned and unrepaired vulnerabilities, failure to handle data security incidents according to legal requirements, and illegal provision of critical data to foreign entities.

To address these trends, we recommend that data controllers:

1) Build a comprehensive data security management system from organizational structure, management processes, and technical measures. The system should cover every phase of the data lifecycle to ensure strict compliance with the PIPL and other relevant laws during data collection, storage, transmission, processing, sharing, and deletion.
2) Regularly conduct data security awareness training for employees and reasonably define personal information processing operation permissions to minimize non-compliance incidents caused by human factors.
3) Establish a robust data security emergency response mechanism and conduct regular drills to ensure rapid and effective responses to unforeseen events. Ensure that when security incidents (such as data breaches) occur, the company can quickly take corrective measures and communicate with regulators or affected individuals as required by law.
4) Carry out data inventory, data classification and grading, personal information protection audits, key data, AI compliance and governance, and cross-border data transfer tasks (detailed below).

2. Data Inventory and Data Classification and Grading

Data inventory and data classification and grading are not new compliance obligations, but through our work with clients, we have found that even as we approach 2025, many companies have yet to complete a data inventory, let alone classify and grade their data.

We highlight data inventory and data classification and grading because they are the foundation and starting point for almost all data compliance obligations. If a company doesn't know what data it holds, and the level

and sensitivity of that data, tasks such as developing privacy policies, managing data transfers, or conducting personal information compliance audits cannot be effectively advanced. Companies that have a solid data inventory and data classification and grading system tend to perform other data compliance tasks more efficiently.

Therefore, we recommend all data controllers (especially those that process personal information and important data), regardless of any specific and special data compliance obligations they have, to conducting and complete data inventory and data classification and grading.

Compared to data inventory, many companies find data classification and grading more abstract and may not know where to start. Here are some suggestions:

1) Complete a data inventory and form a data list detailing each data field.
2) Develop data classification and grading logic tailored to the industry and business specifics of the company. Companies can refer to applicable national or industry standards for the classification and grading logic for their business sectors. For example, financial institutions can refer to the *Financial Data Security - Guides of Data Security Classification*; pharmaceutical companies can refer to the *Information Security Technology - Guide for Health Data Security*; and if no specific classification and grading guidelines are available for an industry, enterprises can refer to documents like *Industrial Data Classification and Grading Guidelines (Draft)* or *Cybersecurity Standards Practice Guidelines - Network Data Classification and Grading Instructions*. Please note that these guidelines are limited in scope and may not necessarily cover all data types of a company, and company will have to develop their own logic and strategies for the classification of data not covered.
3) Use automated tools for data classification and grading, importing the data list to generate an initial classification and grading list. If the data set is small, a manual process can be used to classify and grade according to the established logic.
4) Review the initial classification and grading list and adjust the logic for classifications that do not meet legal and company requirements; then repeat step 3).
5) Form the final data classification and grading list and maintain and update it regularly.

3. Personal Information Protection Audit

Personal information audits have been officially recognized as a legal obligation under the PIPL. Since the publication of draft regulations and national standards such as the *Personal Information Protection Compliance Audit Management Measures* and the *Data Security Technology - Personal Information Protection Compliance Audit Requirements*, the implementation of personal information audits has become feasible. With the *Regulations on Network Data Security Management* reiterating the importance of personal information audits, personal information audits will become an obligation that companies must pay close attention to in 2025.

Every personal information controller must conduct at least one personal information audit every two years, while the following two categories of handlers are required to conduct audits annually:

1) Personal information controllers that process information of more than 1 million individuals.
2) Personal information controllers that process the information of minors.

The data inventory and data classification and grading mentioned in Section 2 above will form the basis for personal information audits. By conducting a comprehensive data inventory and classifying and grading the data, companies can provide clear direction for the audit and ensure that the audit is focused and effective. Key areas of the audit include:

1) The legal basis for personal information processing: Consent? Necessity for contract performance? Legal obligations?
2) Rules for personal information processing: Form and content, and whether notification obligations are fulfilled.
3) Special circumstances for personal information processing: Joint processing, contracted processing, providing information to third parties, data transfer in mergers or splits, automated decision-making, public disclosure, handling sensitive personal information, processing personal information of children under 14, providing personal information abroad.
4) Safeguarding the rights of personal information subjects: Protection of specific rights and responses to rights requests.
5) The effectiveness of personal information protection systems and organizational structure.
6) The technical measures taken for personal information protection.
7) Response to personal information security incidents: Emergency plans and responses.
8) Special audit points for large internet platforms: Independent institutions, platform rules, oversight of platform operators, and social responsibility reports.

We recommend data controllers to plan their 2025 personal information audits promptly, because the process of rectifying non-compliance issues identified in a compliance audit is time consuming and if a controller fails to rectify non-compliance in a timely manner, or encounters regulatory investigations during its rectification, it will nonetheless be regarded to have committed a violation.

4. Important Data Identification and Obligations

The definition of important data and its associated compliance obligations are well understood by most readers, so we will not repeat them here. Instead, this section focuses on why most businesses need to start identifying important data and its related compliance requirements in 2025.

First, the *Data Security Law*, *Regulations on Network Data Security Management*, and other laws and regulations have clarified that important data will be determined by local and industry-specific authorities, who will publish important data catalogs. Businesses will then need to identify, declare, and protect important data according to this catalog. In theory, companies are only required to identify and protect important data once the relevant industry authority has issued the catalog.

However, for the following reasons, we recommend that businesses begin preparing for important data compliance obligations at this stage:

1) **Lead-time for Compliance Obligations**: Once a company is identified as handling important data, it will be subject to numerous compliance obligations, including establishing cybersecurity management bodies and personnel, conducting special risk assessments and annual risk assessments for important data processing, ensuring local storage of important data, and conducting security assessments for cross-border data transfers. These obligations require substantial preparation time and financial investment. Therefore, delaying preparation until the publication of applicable important data catalogs could result in non-compliance for a long time while the company prepares for the implementation of such obligations.

   For example, in terms of data localization, most multinational companies currently use foreign IT systems, and their data typically flows abroad directly rather than being stored domestically. If a company handles important data, it will need to ensure domestic storage for this data, and in some cases, certain data may no longer be allowed to leave the country. This will necessitate a major adjustment of IT systems and business structures. Based on our experience, these adjustments typically take at least six months and require an investment of several million dollars. Therefore, if a company does not plan ahead for its IT system adjustment, it may find itself in a dilemma when important data catalogs are published - either continuing to unlawfully transfer important data abroad or halting data exports, which could disrupt business operations.

2) **Pre-emptive Industry Directives**: Authorities of some highly regulated industry have already issued important data catalogs to companies within the industry through internal meetings and other channels. Although these unpublished catalogs do not carry legal enforceability in theory, the regulatory authorities have required companies to report important data based on these internal catalogs and have specifically emphasized the obligation for companies to conduct security assessments for the cross-border transfer of such important data.

Given these considerations, we recommend that businesses conduct a preliminary assessment of whether they are likely to possess important data. This assessment can be performed concurrently with the data inventory and classification and grading work discussed earlier. It will help determine whether the business will need to fulfill important data obligations in the future.

Recommendations for preliminary assessment:

1) **Complete data inventory**: Start by completing a data inventory, and then identify important data based on this inventory.
2) **Assess according to previous important data standards**: Use important data identification criteria (such as "consequence testing") and relevant national standards and guidelines (including but not limited to the *Information Security Technology - Important Data Identification Guidelines (Draft)*,

Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment, and *Data Security Technology - Rules for Data Classification and Grading* Appendix G, "Important Data Identification Guidelines") to evaluate whether the business's data could harm national security or public interests in the event of a security breach.

3) **Consider aggregated data**: Besides assessing individual fields, consider whether aggregated or combined data could form important data.
4) **Set thresholds for consequence testing**: Businesses should define a "probability" threshold for determining whether specific data constitutes important data. For example, if the threshold is set at 50%, then data with a lower likelihood of harm would not be considered important data. For cases where it is difficult to quantify the probability, qualitative analysis is also recommended.
5) **Consult authorities**: If necessary, seek advice from industry regulators during the process of identifying important data.

5. AI Compliance and Governance

As more companies enter the fields of large language models, AIGC (AI-generated content), and other AI-driven products, AI compliance and governance have become key elements of data compliance work. AI compliance and governance can be divided into two aspects: for service providers and for users. The following are specific compliance recommendations:

As an AI Service Provider:

1) **Algorithm Filing and Security Assessment**: If offering AI services to the public, the provider must file the algorithm with the relevant authorities and conduct security assessments in accordance with national regulations. If the underlying technology relies on third-party large models or algorithms, ensure that the suppliers have completed the necessary filing and assessments.
2) **Regular Audits and Assessments**: Periodically audit, assess, and validate the algorithm mechanisms, models, data, and application outcomes to ensure they do not harm national security, public interests, or disrupt the economic or social order.
3) **Technology Ethics Governance**: Refer to the *Guiding Opinions on Strengthening the Governance of Scientific and Technological Ethics (Draft)*, and based on the business model, establish rules for technological ethics review.
4) **User Management**: Strengthen real-name verification of users, and implement content moderation in line with the *Regulations on the Ecological Governance of Online Information Content* and other relevant laws.
5) **Transparency**: Disclose the basic principles, purposes, and operational mechanisms of the AI service, provide an option to disable AI services, and allow users to manage or delete personal tags used for AI recommendations.
6) **Prevent Misuse**: Avoid abusing big data analytics to set unfair transaction conditions based on user consumption records, preferences, etc.

As an AI User:

1) **Manual Review**: Manually screen and verify the input and output of AI tools to ensure compliance with relevant laws and regulations.
2) **Vendor Assessment**: Before engaging an AI service provider, assess whether they have the necessary qualifications and security capabilities.
3) **Internal Review**: Avoid publishing AI-generated content publicly without appropriate internal review.
4) **Develop AI Usage Guidelines**: Establish AI management policies and usage manuals, and educate employees to avoid inputting sensitive data, such as business secrets, into AI systems.
5) **Monitoring and Reporting**: Set up a monitoring and reporting system to track employee usage of AI tools.
6) **VPN Usage for Foreign AI Services**: When using foreign AI services, ensure that VPN usage is facilitated by a qualified service provider.

6. Data Export

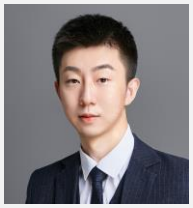
Since the *Regulations on the Promotion and Standardization of Cross-Border Data Flow* came into effect in March this year, China's data export regulatory framework has largely been established. Most businesses involved in data export have already completed the required security assessments or standard contract filings for data export.

For businesses that have not yet fulfilled their data export legal obligations but have data export needs, we recommend the following evaluations in 2025:

1) **Exemption analysis**: Determine if data export scenarios fall under statutory exemptions, such as "necessity for contract performance" or "cross-border human resources management". If all export scenarios can be classified as exempt, no further legal obligations are required; if not, proceed to the next step.
2) **"Positive List" check**: If data export scenarios do not fall under exemptions, check whether they are covered by the "positive list" of a free trade zone (e.g., Shanghai FTZ Lingang Area's general data list). If included, compliance requirements should be met based on the list; if not, proceed to the next step.
3) **Threshold analysis (a)**: For non-exempt export scenarios, determine whether the cumulative number of personal data subjects exported to foreign entities exceeds 100,000, or if any sensitive personal data is involved. If not, no further legal obligations are required; if so, proceed to the next step.
4) **Threshold analysis (b)**: For non-exempt export scenarios, determine whether the cumulative number of personal data subjects exported to foreign entities exceeds 1 million, or if sensitive personal data exceeding 10,000 individuals is involved. If so, conduct a security assessment; if not, conduct the standard contract filing or the certification of personal information protection.
5) **Important data export**: If the relevant industry authority or other government departments have issued an important data catalog, assess whether the business handles important data and whether any exported data falls under this category. If so, conduct a security assessment for important data export.

We hope this Client Alert helps you better plan your data compliance objectives and tasks for 2025. If you would like to learn more about data inventories, classification and grading, personal information protection audits, important data, AI compliance and governance, data export, or any other cybersecurity and data-related legal services, please feel free to contact us:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD