

---

## REGULATORY OVERVIEW

---

### REGULATIONS ON CORPORATION AND FOREIGN INVESTMENT

#### The Company Law

On December 29, 1993, the Standing Committee of the National People’s Congress (the “SCNPC”) promulgated the Company Law of the PRC (《中華人民共和國公司法》), which came into effect on July 1, 1994 (subsequently amended on December 25, 1999, August 28, 2004, October 27, 2005, December 28, 2013, October 26, 2018 and December 29, 2023 (the latest amendments became effective on July 1, 2024)), provides that companies established in China may take the form of limited liability company or a company limited by shares. Each company has the status of a legal person and owns its assets in its own name. The Company Law applies to foreign-invested companies unless relevant laws provide otherwise.

#### FOREIGN INVESTMENT

Investment in the PRC by foreign investors are mainly regulated by the Catalog of Industries for Encouraging Foreign Investment (2022 Edition) (《鼓勵外商投資產業目錄》(2022年版)), which was promulgated by the Ministry of Commerce of the PRC (the “MOFCOM”) and the National Development and Reform Commission of the PRC (the “NDRC”) on October 26, 2022 and took effect on January 1, 2023, and the Special Administrative Measures for Access of Foreign Investment (Negative List) (2024 Edition) (《外商投資准入特別管理措施(負面清單)》(2024年版)) (the “**Negative List**”), which were promulgated by the MOFCOM and the NDRC on September 6, 2024 and took effect on November 1, 2024. The Negative List sets out several restrictive measures in a unified manner, such as the requirements on shareholding percentages and management, for the access of foreign investments in the industries listed in the Negative List and the industries that are prohibited for foreign investment. Any industries not falling in the Negative List shall be administered under the principle of equal treatment to domestic and foreign investment. On March 15, 2019, the NPC promulgated the Foreign Investment Law of the PRC (《中華人民共和國外商投資法》) (the “**FIL**”), which came into effect on January 1, 2020, pursuant to which, it is applicable to the investment activities in the PRC carried out directly or indirectly by foreign natural persons, enterprises or other organizations. The Implementation Rules to the Foreign Investment Law of the PRC (《中華人民共和國外商投資法實施條例》), which were promulgated by the State Council on December 26, 2019 and became effective on January 1, 2020, further clarify that the state encourages and promotes foreign investment, protects the lawful rights and interests of foreign investors, regulates foreign investment administration, continues to optimize foreign investment environment, and advances a higher-level opening.

On December 30, 2019, the MOFCOM and the SAMR jointly promulgated the Measures for Information Reporting on Foreign Investment (《外商投資信息報告辦法》), which became effective on January 1, 2020, pursuant to which, where a foreign investor carries out investment activities in the PRC directly or indirectly, the market regulatory authorities shall forward the investment information submitted by foreign investor or the foreign-invested enterprise to the competent commerce administrative authorities.

### LAWS AND REGULATIONS ON CYBERSECURITY, DATA SECURITY AND PERSONAL INFORMATION PROTECTION

#### Cybersecurity and Data Security

The PRC regulatory authorities have enacted laws and regulations concerning internet information security and the protection of personal data against misuse or unauthorized disclosure, and which includes the Decisions on Protection of Internet Security (《全國人民代表大會常務委員會關於維護互聯網安全的決定》) enacted and amended by the NPCSC on December 28, 2000 and August 27, 2009, respectively, the Provisions on the Technical Measures for Internet Security Protection (《互聯網安全保護技術措施規定》) issued by the Ministry of Public Security (the “MPS”) on December 13, 2005 and became effective on March 1, 2006, the Decision of the Standing Committee of the National People’s Congress on Strengthening Network Information Protection

---

## REGULATORY OVERVIEW

---

(《全國人民代表大會常務委員會關於加強網絡信息保護的決定》) promulgated by the NPCSC on December 28, 2012, the Several Provisions on Regulating the Market Order of Internet Information Services(《規範互聯網信息服務市場秩序若干規定》) promulgated by the Ministry of Industry and Information Technology of PRC (the “MIIT”) on December 29, 2011.

On June 22, 2007, MPS, National Administration of State Secrets Protection and other governmental authorities issued the Administrative Measures for the Graded Protection of Information Security (《信息安全等級保護管理辦法》), which regulates that the security protection of an information system may be graded into five. For an information system of Grade II or above newly built, its operator or user shall, within 30 days after it is put into operation, complete the record filing procedures at the local public security organ at the level of municipality divided into districts or above.

On July 1, 2015, the NPCSC issued the National Security Law of the People’s Republic of China (《中華人民共和國國家安全法》), which came into effect on the same day, pursuant to which the State shall safeguard the sovereignty, security and development interests of the state cybersecurity, and that the State shall establish a national security review and supervision system to review, among other things, foreign investment, key technologies, internet and information technology products and services, and other important activities that are likely to impact the national security of the PRC.

On November 7, 2016, the NPCSC promulgated the Cybersecurity Law of the People’s Republic of China (《中華人民共和國網絡安全法》) (the “**Cybersecurity Law**”), which became effective on June 1, 2017. The Cybersecurity Law applies to the construction, operation, maintenance and use of networks as well as the supervision and administration of cyber security in the PRC. According to the Cybersecurity Law, network operators are broadly defined as owners and administrators of networks and network service providers, and such network operators shall comply with laws and regulations and fulfill their obligations to safeguard security of the network when conducting business and providing services. Those who construct or operate networks or provide services through networks shall take technical measures and other necessary measures pursuant to the mandatory requirements of laws, regulations and national standards to safeguard the safe and stable operation of the networks, respond to network security incidents effectively, prevent illegal and criminal activities, and maintain the integrity, confidentiality and usability of network data. On October 28, 2025, the NPCSC further revised the Cybersecurity Law, which became effective on January 1, 2026. The revised Cybersecurity Law stipulates that, among others, the state supports basic theoretical research on artificial intelligence and the research of key technologies such as algorithms, promotes the construction of infrastructure for training data resources and computing power, improves AI ethical standards, strengthens risk monitoring, assessment, and security supervision, and facilitates the application and healthy development of artificial intelligence. The revised Cybersecurity Law also increases penalties under certain circumstances such as failure to discharge the obligation of safeguarding cybersecurity, and failure to take actions against information that is prohibited from being published or disseminated by laws or administrative regulations, and expands extraterritorial application for entities, organizations, or individuals outside the PRC engaging in activities that endanger the cybersecurity of the PRC.

On June 10, 2021, the NPCSC promulgated the Data Security Law of the People’s Republic of China (《中華人民共和國數據安全法》) (the “**Data Security Law**”), which became effective on September 1, 2021. According to the Data Security Law, “data” is defined as any record of information in electronic or other forms, and the processing activities of data includes the collection, storage, use, processing, transmission, provision and disclosure of data. The Data Security Law is broadly applicable to such processing activities of data which are carried out in the PRC or, where carried out outside the PRC, damage the national security, public interests or the legitimate rights and interests of citizens and organizations of the PRC. The Data Security Law mainly sets forth specific provisions regarding establishing basic systems for data security management, including a data classification and hierarchical protection system, risk assessment system, monitoring and early

---

## REGULATORY OVERVIEW

---

alert system, and emergency disposal system. In addition, it clarifies the data security protection obligations of organizations and individuals carrying out data processing activities and implementing data security protection responsibility, including without limitation, that any organization or individual collecting data shall adopt lawful and proper methods and shall not acquire data by theft or in other illegal manners, and risk monitoring shall be strengthened when data processing activities are carried out, and where risks such as data security flaws and vulnerabilities are discovered, remedial measures shall be immediately taken.

On July 6, 2021, the General Office of the Central Committee of the Communist Party of China, and the General Office of the State Council jointly issued the Opinions on Strictly Combatting Illegal Securities Activities in Accordance with the Law (《關於依法從嚴打擊證券違法活動的意見》). The opinions emphasized the need to strengthen the administration over illegal securities activities and the supervision on overseas listings by China-based companies and improve the legislation on data security, cross-border data transmission, and confidential information management.

On July 30, 2021, the State Council promulgated the Regulations of Security Protection for Critical Information Infrastructure (《關鍵信息基礎設施安全保護條例》) (the “**CII Protection Regulations**”), which became effective on September 1, 2021. Pursuant to the CII Protection Regulations, critical information infrastructure refers to important network infrastructure and information systems of important industries and fields such as public communications and information services, energy, transportation, water conservancy, finance, public services, e-government affairs and national defense science, and other important ones whose damage, function loss or data leakage may endanger national security, people’s livelihood and public interests. According to the CII Protection Regulations, the competent administrative departments and supervisory departments, which govern each respective important industry or field, shall be responsible for formulating the identification rules on and organizing the identification of the critical information infrastructure in such industry or field, and such departments should promptly notify the critical information infrastructure operator (the “**CIIO**”) of the identification results.

On December 28, 2021, the CAC and other 12 PRC regulatory authorities jointly revised and promulgated the Measures for Cybersecurity Review (《網絡安全審查辦法》) (the “**Revised Measures for Cybersecurity Review**”), which became effective on February 15, 2022. The Revised Measures for Cybersecurity Review provides that, among others, (i) a CIIO purchasing network products and services or a network platform operator that engages in data processing activities that affect or may affect national security shall be subject to the cybersecurity review by the Cybersecurity Review Office, the department which is responsible for the implementation of cybersecurity review under the CAC; (ii) a network platform operator with personal information of more than one million users which seeks listing in a foreign country is obliged to apply for a cybersecurity review by the Cybersecurity Review Office; and (iii) the relevant regulatory authorities may initiate cybersecurity review if such regulatory authorities determine that the issuer’s network products or services, or data processing activities affect or may affect national security.

On July 7, 2022, the CAC promulgated the Measures for the Security Assessment of Cross-border Data Transfer (《數據出境安全評估辦法》) (the “**Security Assessment Measures**”), which became effective on September 1, 2022. The Security Assessment Measures applies to the security assessment conducted by data processors where they provide overseas parties with important data or personal information collected and generated during operations within the territory of the PRC. Based on the Security Assessment Measures, data processors shall apply to the CAC through the provincial cyberspace administration in the place where they operate for a security assessment of cross-border data transfer if such transfer is conducted by a CIIO, or involves important data, or their cross-border data transfer activities fulfill certain thresholds.

---

## REGULATORY OVERVIEW

---

On June 27, 2022, the CAC promulgated the Administrative Provisions on the Account Information of Internet Users (《互聯網用戶帳號信息管理規定》), which became effective on August 1, 2022. The obligations of internet-based information service providers include but not limited to: (i) authenticate the identity information of the users who apply for registration of relevant account and verify the account information submitted by users upon registration; (ii) display the location information of IP addresses of internet users’ accounts on the information page of internet users’ accounts; and (iii) equip themselves with professional and technical capabilities appropriate to the scale of services.

On December 8, 2022, the MIIT issued the Administrative Measures for Data Security in the Industrial and Information Technology Field (Trial Implementation) (《工業和信息化領域數據安全管理辦法(試行)》) (the “**MIIT Data Security Measures**”), which came into effect on January 1, 2023. The MIIT Data Security Measures is applicable to the processing activities carried out in the territory of the PRC of data in the field of industry and information technology, which include, among other things, the data collected and generated in the course of research, development and design, production and manufacturing, operation and management, operating and maintenance and platform operation in the field of industry. The MIIT Data Security Measures provides that industrial and telecommunication data processors shall implement data classification and grading, and further imposes data security obligations and responsibilities on data processors in the field of industry and information technology, which include, among others, taking protective measures based on the corresponding grading of data, establishing management system covering the whole data lifecycle, and staffing data security management personnel as needed to be in charge of the security supervision and management of data processing activities as a whole and assisting with the industrial administrative authorities in carrying out the relevant work.

On March 22, 2024, the CAC promulgated the Provisions on Promoting and Regulating Cross-Border Data Flow (《促進和規範數據跨境流動規定》), effective on the date of promulgation. The provisions provide several exemptions to data processors which exempt them from undergoing data security assessment, obtaining personal information protection certification, or entering into standard contracts for outbound transfer of personal information for businesses. These exemptions include, among others, scenarios where a data processor, other than a CIIO, has cumulatively transferred personal information (excluding sensitive personal information) of fewer than 100,000 individuals to overseas recipients since January 1 of the current year. In addition, a data processor, other than a CIIO, shall enter into a standard contract with overseas recipients for the cross-border transfer of personal information, or obtain certification for personal information protection if, since January 1 of the current year, the data processor has cumulatively transferred to overseas recipients personal information (excluding sensitive personal information) of more than 100,000 but fewer than 1,000,000 individuals, or sensitive personal information of fewer than 10,000 individuals. The provisions also explicitly state that data processors are not required to apply for security assessment on cross-border transfer of important data, provided that the relevant data has not been notified or published as important data by relevant departments or regions.

On September 24, 2024, the Administration Regulations on Cyber Data Security (《網絡數據安全管理條例》) (the “**Regulation on Cyber Data Security**”) was issued by the State Council, which became effective on January 1, 2025. The Regulation on Cyber Data Security provides that cyber data processors whose cyber data processing activities affect or may affect national security shall be subject to national security review in accordance with the relevant regulations. In addition, the Regulations on Cyber Data Security also regulate other specific requirements in respect of the cyber data processing activities conducted by data processors in the view of, among others, personal information protection, important data safety, and cyber data cross-border safety management and obligations of network platform service provider.

---

## REGULATORY OVERVIEW

---

### Personal Information Protection

On July 16, 2013, the MIIT promulgated the Regulations on Protection of Personal Information of Telecommunications and Internet Users (《電信和互聯網用戶個人信息保護規定》), which came into effect on September 1, 2013, to enhance and enforce legal protection over user information security and privacy on the internet. The Regulations on Protection of Personal Information of Telecommunications and Internet Users require internet operators to take various measures to ensure the privacy and confidentiality of users’ information.

On August 29, 2015, the NPCSC issued the Ninth Amendment to the Criminal Law of the People’s Republic of China (《中華人民共和國刑法修正案(九)》), which became effective on November 1, 2015, stipulates that any network service provider that fails to fulfill the obligations related to information network security management as required by applicable laws and administrative regulations and refuses to take corrective measures after the regulatory authorities order them to correct the non-performance, shall be subject to criminal liability for causing (i) any large-scale dissemination of illegal information; (ii) any serious consequence due to the leakage of users’ information; (iii) any serious loss of evidence of criminal activities or (iv) other serious circumstances, and any individual or entity that (a) sells or provides personal information to others unlawfully or (b) steals or illegally obtains any personal information will be subject to criminal liability in serious circumstances. Pursuant to the Notice of the Supreme People’s Court, the Supreme People’s Procuratorate and the Ministry of Public Security on Legally Punishing Criminal Activities Infringing upon the Personal Information of Citizens (《最高人民法院、最高人民檢察院、公安部關於依法懲處侵害公民個人信息犯罪活動的通知》), issued on April 23, 2013, and the Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues regarding Legal Application in Criminal Cases Infringing upon the Personal Information of Citizens (《最高人民法院、最高人民檢察院關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》), which was issued on May 8, 2017 and became effective on June 1, 2017, the following activities may constitute the crime of infringing upon a citizen’s personal information: (i) providing a citizen’s personal information to specified persons or releasing a citizen’s personal information online or through other methods in violation of relevant national provisions; (ii) providing legitimately collected information relating to a citizen to others without such citizen’s consent (unless the information is processed, not traceable to a specific person and not recoverable); (iii) collecting a citizen’s personal information in violation of applicable rules and regulations when performing a duty or providing services; or (iv) collecting a citizen’s personal information by purchasing, accepting or exchanging such information in violation of applicable rules and regulations.

On May 28, 2020, the NPC promulgated the Civil Code of the People’s Republic of China (《中華人民共和國民法典》) (the “**Civil Code**”). Pursuant to the Civil Code, the personal information of a natural person shall be protected by the law. Any organization or individual that needs to obtain personal information of others shall obtain such information legally and ensure the safety of such information, and shall not illegally collect, use, process or transmit personal information of others, or illegally purchase or sell, provide or make public personal information of others.

On August 20, 2021, the NPCSC promulgated the Personal Information Protection Law of the People’s Republic of China (《中華人民共和國個人信息保護法》) (the “**Personal Information Protection Law**”), which became effective on November 1, 2021. Pursuant to the Personal Information Protection Law, the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information, and before processing personal information, personal information processors should truthfully, accurately and completely inform individuals of the following matters in a conspicuous manner and in clear and easy-to-understand language: (i) the name and contact information of the personal information processor; (ii) purpose of processing personal information, processing method, type of personal information processed and retention period; (iii) methods and procedures for individuals to exercise their rights under the Personal Information Protection Law; and (iv) other matters that should be notified as required by laws and administrative regulations. Personal information

---

## REGULATORY OVERVIEW

---

processors should also take the following measures to ensure that personal information processing activities comply with laws and administrative regulations based on the processing purpose, processing methods, types of personal information, impact on personal rights and interests, and possible security risks, etc., and to prevent unauthorized access and personal information leakage, tampering and loss: (i) formulating internal management systems and operating procedures; (ii) implementing classified management of personal information; (iii) adopting corresponding security technical measures such as encryption and de-identification; (iv) reasonably determining the operating authority for personal information processing, and regularly conduct safety education and training for practitioners; (v) formulating and organizing the implementation of emergency plans for personal information security incidents; and (vi) other measures stipulated by laws and administrative regulations.

Where personal information is processed in violation of the provisions of the Personal Information Protection Law, or the processing of personal information fails to fulfill the personal information protection obligations hereunder, the department performing personal information protection duties shall order corrections, give warnings, confiscate illegal gains, and order to suspend or terminate the provision of services by the applications that illegally process personal information; if the personal information processor refuses to make corrections, a fine of not more than RMB1 million shall be imposed; the directly responsible person in charge and other directly responsible personnel shall be fined not less than RMB10,000 but not more than RMB100,000. For any aforesaid illegal act with serious circumstances, the department performing personal information protection duties at or above the provincial-level shall order the personal information processor to make corrections, confiscate the illegal gains, and impose a fine of less than RMB50 million or less than 5% of the previous year’s turnover. It can also order the suspension of relevant business or suspend business for rectification, notify the relevant competent authority to revoke the relevant permits or the business license; impose a fine of RMB100,000 up to RMB1 million on the directly responsible person in charge and other directly responsible personnel, and may decide to prohibit them from serving as a director, supervisor, senior manager and person in charge of personal information protection of related companies within a certain period of time.

On February 22, 2023, the Measures for the Administration of Standard Contractual Clauses for the Cross-Border Transfer of Personal Information (《个人信息出境标准合同办法》), were promulgated by the CAC, which became effective on June 1, 2023 and provide requirements and guidelines for personal information processors to enter into a contract for outbound transfer of personal information abroad and conduct relevant filing procedures.

On February 12, 2025, the Administrative Measures for the Compliance Audit of Personal Information Protection (《个人信息保护合规审计管理办法》), was promulgated by the CAC, which became effective on May 1, 2025. According to the Administrative Measures for the Compliance Audit of Personal Information Protection, the term “compliance audit of personal information protection” refers to supervisory activities that review and evaluate whether the personal information processing activities of personal information processors comply with laws and administrative regulations. Personal information processors that process the personal information of more than 10 million individuals shall carry out the compliance audit of personal information protection at least every two years. Personal information processors in any of the following circumstances may be required by the CAC and other authorities performing personal information protection duties to entrust a professional agency to conduct a compliance audit of their personal information processing activities: (1) where significant risks are identified in the personal information processing activities that severely impact individual rights or lack adequate security measures; (2) where the personal information processing activities may infringe upon the rights and interests of a large number of individuals; (3) in the event of a personal information security incident resulting in the leakage, tampering, loss, or destruction of personal information of more than 1 million individuals or sensitive personal information of more than 100,000 individuals.

---

## REGULATORY OVERVIEW

---

### Algorithm and Generative AI Services Governance

On December 31 2021, the CAC, the MIIT, MPS, the SAMR jointly promulgated the Administrative Provisions on Internet Information Service Algorithm Recommendation (《互聯網信息服務算法推薦管理規定》), which became effect on March 1, 2022. The Administrative Provisions on Internet Information Service Algorithm Recommendation implements classification and hierarchical management for algorithm recommendation service providers based on various criteria, and stipulates that algorithm recommendation service providers with public sentiment attributes or social mobilizing capability shall file with the CAC within ten business days from the date of providing such services.

On November 25, 2022, the CAC, MIIT and MPS promulgated the Administrative Provisions on Deep Synthesis of Internet Information Service (互聯網信息服務深度合成管理規定), which took effect on January 10, 2023. The “deep synthesis technology” provided in such provisions refers to the technology to generate text, graphics, radio, video, virtual scenes, among others, with the use of deep learning and virtual reality. The measures emphasize that the deep synthesis services shall not be utilized for illegal activities prohibited by laws and regulations, and specifically, the related providers of such deep synthesis services shall (i) establish and improve control systems in regard to user registration, algorithm review, technological ethic review, information public review, data security, personal information protection, anti-telecom and online fraud, emergency disposal, etc. and hold safe and controlled technical protection measures; (ii) formulate and publicize related management rules and platform pacts, improve service agreements, perform management responsibilities in accordance with laws and agreements, and inform with explicit methods the technical supporters and users of the deep synthesis of their respective information safety obligations.

On July 10, 2023, the CAC together with other relevant authorities, released the Provisional Administrative Measures for Generative Artificial Intelligence Services (《生成式人工智能服務管理暫行辦法》) (“**Generative AI Services Measures**”), which came into effect on August 15, 2023 and mainly impose compliance requirements on providers of generative AI services. According to the Generative AI Services Measures, individuals or organizations that provide generative AI services of text, image, audios, videos and other content shall be responsible as the producers of such network information content and as the personal information processors to protect any personal information involved. Providers of generative AI services shall enter into service agreements with users registering for their generative AI services and shall adopt effective measures to prevent minor users from over-relying or addicting to generative AI services. In the event where illegal content or users engaging in illegal activities using generative AI services are discovered, the generative AI services providers are required to take appropriate measures, including stopping the generation of such illegal content and suspending or terminating the provision of services, undergo rectifications, keep relevant records and report to the competent authority. Any provider of generative AI services with public sentiment attributes or social mobilizing capability shall conduct security assessment and complete certain filings in accordance with relevant regulations. Providers of generative AI services may be subject to penalties for non-compliance, including warning, public denouncement, rectification orders and suspension of the provision of relevant services.

On March 7, 2025, the CAC, the MIIT, the MPS and the National Radio and Television Administration jointly issued the Notice on Promulgation of the Measures for Labeling AI-Generated or Composed Content (《人工智能生成合成內容標識辦法》), which will become effective on September 1, 2025, pursuant to which, internet information service providers have the obligations to add explicit or implicit labels to the AI-generated or composed content in certain circumstances.

On March 20, 2026, the MIIT and nine other relevant authorities jointly promulgated the Measures for Ethical Review and Services of Artificial Intelligence Technologies (for Trial Implementation) (《人工智能科技倫理審查與服務辦法(試行)》) (the “**AI Ethical Review Measures**”), which came into effect on the same day. Key AI activities, which includes, amongst others, the R&D

---

## REGULATORY OVERVIEW

---

of algorithm models, applications and systems with public opinion/social mobilization capability and social consciousness-guiding capability, and R&D of automated decision-making systems with a high degree of autonomy for scenarios with safety or personal health risks, are subject to additional expert review. Relevant entities must also complete and update required registrations on the National Science and Technology Ethics Management Information Registration Platform.

### REGULATIONS RELATING TO EMPLOYMENT AND SOCIAL WELFARE

#### The Labor Contract Law

The Labor Law of the PRC (《中華人民共和國勞動法》), effective January 1, 1995 and most recently amended on December 29, 2018, along with the Labor Contract Law of the PRC (《中華人民共和國勞動合同法》), effective January 1, 2008 and amended on December 28, 2012, collectively establish the mandatory requirement that formal labor contracts must be executed between employers and employees to establish lawful employment relationships within the PRC. The Interim Provisions on Labor Dispatch (《勞務派遣暫行規定》), effective March 1, 2014, further limit the number of dispatched workers to no more than 10% of an enterprise’s total workforce, and the aforementioned total workforce refers to the sum of the number of people who have signed labor contracts with the employing unit and the number of dispatched workers who have been employed.

#### Social Insurance and Housing Provident Fund

The Social Insurance Law of the PRC (《中華人民共和國社會保險法》), promulgated on October 28, 2010 and effective July 1, 2011, and latest amended on December 29, 2018, along with the Interim Regulations on the Collection of Social Insurance Fees (《社會保險費徵繳暫行條例》) issued by the State Council on January 22, 1999 and last amended on March 24, 2019, establish the mandatory social insurance participation requirements for employees in the PRC. Under these regulations, employees must participate in three social insurance programs where contributions are shared between employers and employees: basic pension insurance, basic medical insurance, and unemployment insurance. Additionally, employees are covered by two employer-funded programs: work-related injury insurance and maternity insurance. The integration of maternity insurance with basic medical insurance was initiated through the Notice of the General Office of the State Council on Issuing the Plan for the Pilot Program of Combined Implementation of Maternity Insurance and Basic Medical Insurance for Employees (《國務院辦公廳關於印發的通知》) issued on January 19, 2017, and fully implemented nationwide pursuant to the Opinions of the General Office of the State Council on Comprehensively Promoting the Implementation of the Combination of Maternity Insurance and Basic Medical Insurance for Employees (《國務院辦公廳關於全面推進生育保險和職工基本醫療保險合併實施的意見》) promulgated on March 6, 2019. The Social Insurance Law of the PRC mandates employers to complete social insurance registration with local social insurance agencies and fulfill their obligations to either pay or withhold and remit the relevant social insurance premiums on behalf of employees. Noncompliance triggers graduated penalties: employers failing to register for social insurance will be ordered to rectify within a specified period, with potential penalties ranging from one to three times the payable premiums for continued non-compliance. Similarly, delayed or incomplete premium payments incur daily late fees of 0.05% of the outstanding amount from the due date, plus potential fines of one to three times the defaulted amount if not remedied within the prescribed timeframe.

The Regulations on the Administration of Housing Provident Fund (《住房公積金管理條例》), initially promulgated on April 3, 1999 and subsequently amended on March 24, 2002 and March 24, 2019, establish mandatory requirements for housing provident fund contributions in the PRC. Employers are obligated to make full and timely payments of housing provident funds, with express prohibitions against overdue or insufficient payments. Compliance requires employers to complete both payment processing and deposit registration procedures with the designated housing provident fund administrative center. The regulations implement a graduated enforcement mechanism for non-compliance. Enterprises failing to register for housing provident funds or establish employee accounts will receive correction orders from the housing provident fund administrative center, with

---

## REGULATORY OVERVIEW

---

stipulated time limits for compliance. Persistent violations may result in administrative fines ranging from RMB10,000 to RMB50,000. For payment defaults, the administrative center will first issue orders requiring full payment within specified periods. Should enterprises continue non-compliance beyond these deadlines, the regulations authorize the administrative center to petition the People’s Court for compulsory enforcement.

The Reform Plan of the State Tax and Local Tax Collection Administration System (《國稅地稅徵管體制改革方案》), jointly promulgated by the General Office of the Communist Party of China and the General Office of the State Council on July 20, 2018, implemented a fundamental restructuring of social insurance premium collection mechanisms effective January 1, 2019. This reform transferred collection authority for all social insurance programs, including basic pension insurance, unemployment insurance, maternity insurance, work injury insurance, and basic medical insurance, to the tax administration system. Supplementary guidance was provided through two key notices: the Notice of the General Office of the State Taxation Administration on Conducting the Relevant Work Concerning the Administration of Collection of Social Insurance Premiums in a Steady, Orderly and Effective Manner (《國家稅務總局辦公廳關於穩妥有序做好社會保險費徵管有關工作的通知》) issued on September 13, 2018, and the Urgent Notice of the General Office of the Ministry of Human Resources and Social Security on Implementing the Spirit of the Executive Meeting of the State Council in Stabilizing the Collection of Social Insurance Premiums (《人力資源社會保障部辦公廳關於貫徹落實國務院常務會議精神切實做好穩定社保費徵收工作的緊急通知》) issued on September 21, 2018. These documents established strict prohibitions against local authorities conducting retrospective self-collection of historical social insurance arrears from enterprises. This policy direction was reaffirmed in the Notice of the State Administration of Taxation on Implementing the Several Measures to Further Support and Serve the Development of Private Economy (《國家稅務總局關於實施進一步支持和服務民營經濟發展若干措施的通知》) promulgated on November 16, 2018, which explicitly prohibited tax authorities at all levels from initiating retrospective self-collection of overdue premiums from private enterprises or other taxpayers for previous years.

On July 31, 2025, the PRC Supreme People’s Court promulgated the Supreme People’s Court’s Interpretation (II) on Several Issues Concerning the Application of Law in Labor Dispute Cases (《最高人民法院關於審理勞動爭議案件適用法律問題的解釋(二)》), (the “**New Judicial Interpretation**”), which took effect on September 1, 2025. Article 19(1) thereof stipulates that if an employer and an employee agree or the employee undertakes that social insurance contributions need not be paid, the court shall deem such agreement or undertaking invalid. Furthermore, where an employer fails to pay social insurance contributions in accordance with the law, and the employee seeks to terminate the labor contract and claims economic compensation from the employer pursuant to Article 38(3) of the PRC Labor Contract Law, the court shall support such claims in accordance with the law, which clarifies that employees are entitled to request termination of their labor contracts and receive corresponding economic compensation under the PRC Labor Contract Law if the employer fails to make social insurance contributions in accordance with the law.

## REGULATIONS ON INTELLECTUAL PROPERTY IN THE PRC

### Copyright Law and its Implementing Rules of the PRC

On September 7, 1990, the SCNPC promulgated the Copyright Law of the PRC (《中華人民共和國著作權法》) (the “**Copyright Law**”), which was last amended on November 11, 2020 and came into effect on June 1, 2021. The Copyright Law stipulates copyrights include personal rights such as the right of publication and that of attribution as well as property rights such as the right of production and that of distribution. Reproducing, distributing, performing, projecting, broadcasting or compiling a work or communicating the same to the public via an information network without permission from the owner of the copyright therein, unless otherwise provided in the Copyright Law, shall constitute infringements of copyrights. The infringer shall, according to the circumstances of the case, undertake to cease the infringement, take remedial action, and offer an apology, pay damages, etc.

---

## REGULATORY OVERVIEW

---

### Trademark Law and its implementation regulation of the PRC

Trademarks are protected by the Trademark Law of the PRC (《中華人民共和國商標法》) which was promulgated on August 23, 1982 and subsequently amended on February 22, 1993, October 27, 2001, August 30, 2013, April 23, 2019 and took effect on November 1, 2019 as well as the Implementation Regulation of the PRC Trademark Law (《中華人民共和國商標法實施條例》) adopted by the State Council on August 3, 2002 and revised on April 29, 2014. In the PRC, registered trademarks include commodity trademarks, service trademarks, collective marks and certification marks. The Trademark Office of National Intellectual Property Administration handles trademark registrations and grants a term of 10 years to registered trademarks, renewable every 10 years where a registered trademark needs to be used after the expiration of its validity term.

### Patent Law of the PRC

On March 12, 1984, the SCNPC promulgated the Patent Law of the PRC (《中華人民共和國專利法》), which was last amended on October 17, 2020 and came into effect on June 1, 2021. On June 15, 2001, the State Council promulgated the Implementation Rules of The Patent Law of the PRC (《中華人民共和國專利法實施細則》), which was last amended on December 11, 2023 and came into effect on January 20, 2024. Both stipulates that patents in China are divided into invention patent, utility patent and design patent. Invention patent refers to new technical solutions for a product, method or its improvement; utility patent refers to new technical solutions for the shape, structure or the combination of both shape and structure of a product, which is applicable for practical use; design patent refers to new designs of the shape, pattern or the combination of shape and pattern, or the combination of the color, the shape and pattern of a product with esthetic feeling and industrial application value. Invention patent shall be valid for 20 years from the date of application while utility patent shall be valid for ten years from the date of application and design patent shall be valid for fifteen years from the date of application. The patent right entitled to its owner shall be protected by the laws. Any person shall be licensed or authorized by the patent owner before using such patent. Otherwise, the use constitutes an infringement of the patent right.

### Administrative Measures for Internet Domain Names

The MIIT promulgated the Administrative Measures on Internet Domain Names (《互聯網域名管理辦法》) (the “**Domain Name Measures**”) on August 24, 2017, which took effect on November 1, 2017. Pursuant to the Domain Name Measures, the MIIT oversees the administration of PRC Internet domain names. The domain name registration follows a first-to-file principle. Applicants for registration of domain names must provide the true, accurate, and complete information of their identities to domain name registration service institutions. The applicants will become the holder of such domain names upon the completion of the registration procedure.

## REGULATIONS ON TAX IN THE PRC

### Enterprise Income Tax Law

On March 16, 2007, the SCNPC promulgated the Enterprise Income Tax Law of the PRC (《中華人民共和國企業所得稅法》) (the “**EIT Law**”), which was last amended on December 29, 2018 and became effective on the same date. On December 6, 2007, the State Council promulgated the Implementation Rules to the EIT Law (《中華人民共和國企業所得稅法實施條例》) (the “**Implementation Rules**”), which was amended on April 23, 2019. Both stipulates that enterprises are divided into resident enterprises and non-resident enterprises. A resident enterprise shall pay enterprise income tax on its income deriving from both inside and outside China at the rate of enterprise income tax of 25%. A non-resident enterprise that has an establishment or place of business in the PRC shall pay enterprise income tax on its income deriving from inside China and obtained by such establishment or place of business, and on its income which derives from outside China but has actual relationship with such establishment or place of business, at the rate of enterprise income tax of 25%. A non-resident enterprise that does not have an establishment or place

---

## REGULATORY OVERVIEW

---

of business in China, or has an establishment or place of business in China but the income has no actual relationship with such establishment or place of business, shall pay enterprise income tax on its income deriving from inside China at the reduced rate of enterprise income tax of 10%.

### Value-added Tax

Pursuant to Value-added Tax Law of the People’s Republic of China (《中華人民共和國增值稅法》), promulgated on December 25, 2024, and became effective on January 1, 2026, all enterprises and individuals engaged in the sale of goods, the provision of processing, repair and replacement services, sales of services, intangible assets, real property, and the importation of goods within the territory of the PRC shall be liable to pay VAT, the VAT tax rates generally applicable are simplified as 13%, 9%, 6% and 0%, the VAT tax rate applicable to the small-scale taxpayers is 3%. Regulations for the Implementation of the Value-Added Tax Law of the People’s Republic of China (《中華人民共和國增值稅法實施條例》), promulgated on December 25, 2025, and became effective on January 1, 2026 has detailed taxpayers and scope of taxation, clarify the applicable tax rates and determine the calculation methods for tax payable in different situations.

### REGULATIONS ON FOREIGN EXCHANGE IN THE PRC

According to the Foreign Exchange Administration Regulations of the PRC (《中華人民共和國外匯管理條例》) promulgated on January 29, 1996 and amended on January 14, 1997 and August 5, 2008, the RMB is generally freely convertible for current account items, including the distribution of dividends, trade and service related foreign exchange transactions, but not for capital account items, such as direct investment, loan, repatriation of investment and investment in securities outside the PRC, unless the prior approval of the State Administration of Foreign Exchange (the “SAFE”) or its designated banks is obtained.

According to the Notice of the State Administration of Foreign Exchange on Reforming and Regulating Policies on the Control over Foreign Exchange Settlement of Capital Accounts (《國家外匯管理局關於改革和規範資本項目結匯管理政策的通知》) promulgated on June 9, 2016, the settlement of foreign exchange receipts under the capital account (including but not limited to foreign exchange capital and external debts and funds recovered from overseas listing) may convert from foreign currency into RMB on a self-discretionary basis. The ratio of the discretionary exchange rate of foreign exchange receipts under the domestic capital account is tentatively set at 100%. The SAFE may adjust the above ratio in due course according to the balance of payment status.

According to the Notice of the State Administration of Foreign Exchange on Further Promoting Cross-border Trade and Investment Facilitation (《國家外匯管理局關於進一步促進跨境貿易投資便利化的通知》) which was promulgated on October 23, 2019 and amended by SAFE Notice on Further Deepening the Reform to Facilitate Cross-border Trade and Investment (《國家外匯管理局關於進一步深化改革促進跨境貿易投資便利化的通知》) which was promulgated on December 4, 2023, foreign-invested enterprises engaged in noninvestment business are permitted to settle foreign exchange capital in RMB and make domestic equity investments with such RMB funds according to the law on the condition that the current Special Administrative Measures for Access of Foreign Investment (Negative List) are not violated and the relevant domestic investment projects are genuine and in compliance with laws.

### REGULATIONS ON OVERSEAS LISTING

The CSRC promulgated Trial Administrative Measures of the Overseas Securities Offering and Listing by Domestic Companies (《境內企業境外發行證券和上市管理試行辦法》) (the “**Overseas Listing Trial Measures**”) and five relevant guidelines on February 17, 2023, which came into effective on March 31, 2023. The Overseas Listing Trial Measures regulate both direct and indirect overseas offering and listing by PRC domestic companies’ by adopting a filing-based regulatory regime.

---

## REGULATORY OVERVIEW

---

Pursuant to the Overseas Listing Trial Measures, no overseas offering and listing shall be made under any of the following circumstances: (i) where such securities offering and listing is explicitly prohibited by provisions in laws, administrative regulations and relevant state rules; (ii) where the intended securities offering and listing may endanger national security as reviewed and determined by competent authorities under the State Council in accordance with law; (iii) where the domestic company intending to make the securities offering and listing, or its controlling shareholders and the actual controller, have committed crimes such as corruption, bribery, embezzlement, misappropriation of property or undermining the order of socialist market economy during the latest three years; (iv) where the domestic company intending to make the securities offering and listing is suspected of committing crimes or major violations of laws and regulations, and is under investigation according to law, and no conclusion has yet been made thereof; and (v) where there are material ownership disputes over equity held by the domestic company’s controlling shareholder or by other shareholders that are controlled by the controlling shareholder and/or actual controller.

Initial public offerings or listings in overseas markets shall be filed with the CSRC within three business days after the relevant application is submitted overseas. The Overseas Listing Trial Measures also require subsequent reports to be filed with the CSRC upon the occurrence of any of the material events after an issuer has offered and listed securities in an overseas market, such as (i) change of control; (ii) investigations or sanctions imposed by overseas securities regulatory agencies or other relevant competent authorities; (iii) change of listing status or transfer of listing segment; (iv) voluntary or mandatory delisting. Where an issuer’s main business undergoes material changes after overseas offering and listing, and is therefore beyond the scope of business stated in the filing documents, such issuer shall submit to the CSRC an ad hoc report and a relevant legal opinion issued by a domestic law firm within three business days after occurrence of the changes.

Furthermore, on February 24, 2023, the CSRC, together with certain other PRC governmental authorities, promulgated the Provisions on Strengthening Confidentiality and Archives Administration of Overseas Securities Offering and Listing by Domestic Companies (the “**Confidentiality and Archives Administration Provisions**”) (《關於加強境內企業境外發行證券和上市相關保密和檔案管理工作的規定》), which came into effect on March 31, 2023. According to the Confidentiality and Archives Administration Provisions, PRC domestic companies that directly or indirectly conduct overseas offerings and listings, shall strictly abide by applicable PRC laws and regulations on confidentiality when providing or publicly disclosing, either directly or through their overseas listed entities, documents and materials to securities services providers such as securities companies and accounting firms or overseas regulators in the process of their overseas offering and listing. In the event such documents or materials contain state secrets or working secrets of government agencies, the PRC domestic companies shall first obtain approval from competent authorities according to law, and file with the secrecy administrative department at the same level; in the event that such documents or materials, if leaked, will jeopardize national security or public interest, the PRC domestic companies shall strictly fulfill relevant procedures stipulated by applicable national regulations. The PRC domestic companies shall also provide a written statement of the specific state secrets and sensitive information provided when providing documents and materials to securities companies and securities service providers, and the securities companies and securities service providers shall properly retain such written statements for inspection. Furthermore, the Confidentiality and Archives Administration Provisions also provide where overseas securities regulators and relevant competent overseas authorities request to inspect, investigate or collect evidence from PRC domestic companies concerning their overseas offering and listing or their securities firms and securities service providers that undertake securities business for such PRC domestic companies, such inspection, investigation and evidence collection must be conducted under a cross-border regulatory cooperation mechanism, and the CSRC or other competent authorities of the PRC government will provide necessary assistance pursuant to bilateral and multilateral cooperation mechanism. Domestic companies, securities firms and securities service providers shall first obtain approval from the CSRC or other competent PRC authorities before

---

## REGULATORY OVERVIEW

---

cooperating with the inspection and investigation by the overseas securities regulators or competent overseas authority or providing documents and materials requested in such inspection and investigation.

### REGULATIONS ON MANAGEMENT OF LEASE HOUSING IN THE PRC

Pursuant to the Administrative Measures on Leasing of Commodity Housing On December 1, 2010, the Ministry of Housing and Urban-Rural Development promulgated the Administrative Measures on Leasing of Commodity Housing (《商品房屋租賃管理辦法》), effective February 1, 2011, lessors and lessees shall complete property leasing registration and filing formalities within 30 days from execution of the property lease contract with the development (real estate) department of the PRC Government of the centrally-administered municipality, municipality or county where the leased property is located. Organizations who violate the relevant provisions of this regulation shall be ordered by the development (real estate) department of the PRC Governments of centrally-administered municipalities, municipalities or counties to make corrections within a stipulated period; where an organization fails to make corrections within the stipulated period, a fine ranging from RMB1,000 to RMB10,000 shall be imposed.

### U.S. OUTBOUND INVESTMENT RULES

On October 28, 2024, the U.S. Department of the Treasury issued a final rule on the U.S. Outbound Investment Security Program, titled “*Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern*” (the “**Final Rule**”) and codified in U.S. Code of Federal Regulations at 31 C.F.R. Part 850, to implement Executive Order 14105, “*Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern*,” of August 9, 2023. The Final Rule became effective on January 2, 2025 and applies to covered transactions with a completion date on or after that date. It targets certain investments by U.S. persons in entities in “countries of concern” (currently only China, including Hong Kong and Macau) that engage in activities relating to one or more of the following sectors: (i) semiconductors and microelectronics, (ii) quantum information technologies, and (iii) AI systems.

The Final Rule imposes notification or prohibition requirements on a range of direct or indirect investments by U.S. persons in “covered foreign persons.” “Covered transactions” are defined in § 850.210 and include, among other things, U.S. person’s direct or indirect: (i) acquisitions of equity interests or contingent equity interests, (ii) the provision of certain types of debt financing, (iii) conversions of contingent equity interests into equity interests, and (iv) other similar activities. “Covered foreign persons” include persons from a country of concern (i.e., entities with a principal place of business in, headquartered in, or incorporated or otherwise organised under the laws of the PRC, Hong Kong, and/or Macau, as well as entities majority-owned or controlled by individuals or entities from such jurisdictions) that engage in a “covered activity.” “Covered activities” refer, in the context of a particular transaction, to activities falling within the definitions of “notifiable transaction” or “prohibited transaction” under the Final Rule.

Pursuant to § 850.301 of the Final Rule, U.S. persons (defined to include any U.S. citizen, lawful permanent resident, entity organised under U.S. law or the laws of any jurisdiction within the United States (including any foreign branch of any such entity), or any person in the United States) may not engage in a prohibited transaction unless an exemption for that transaction has been granted. “Prohibited transactions” include covered transactions by U.S. persons involving a covered foreign person that engages in, among other activities, the development of any AI system that is: (i) designed to be exclusively used for any military end use, or government intelligence or mass-surveillance end use; or (ii) trained using a quantity of computing power greater than  $10^{25}$  computational operations, or greater than  $10^{24}$  computational operations where the training uses primarily biological sequence data. “Notifiable transactions” include covered transactions by U.S. persons involving a covered foreign person that engages in, among other activities, the development of an AI system that does not meet the criteria for a prohibited transaction but nonetheless is: (i) designed to be used for any military end use, or government intelligence or mass-surveillance end

---

## REGULATORY OVERVIEW

---

use; (ii) intended for cybersecurity applications, digital forensic tools, penetration testing tools, or the control of robotic systems; or (iii) trained using a quantity of computing power greater than  $10^{23}$  computational operations.

The Final Rule provides that “AI system” means: (i) a machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments, which: (a) uses data inputs to perceive real and virtual environments; (b) abstracts such perceptions into models through automated or algorithmic statistical analysis; and (c) uses model inference to make a classification, prediction, recommendation, or decision; and (ii) any data system, software, hardware, application, tool, or utility that operates in whole or in part using a system described in (i) above. “Developing” an AI system is defined in § 850.211 to include engaging in any stages prior to serial production, such as design or substantive modification, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, processes of transforming design data into a product, configuration design, integration design, and layouts. Note 2 to § 850.217 further clarifies that, for purposes of the notification requirement, development requires the Company to engage in one or more of the activities enumerated in § 850.211 (such as design or substantive modification) with respect to the third-party AI model or machine-based system used by a data system, software, hardware, application, tool, or utility that operates in whole or in part using such model or system.

As our business activities involve the development of AI systems within the scope of covered activities that could result in a notifiable transaction (but not a prohibited transaction), we would be considered a “covered foreign person” for purposes of the Final Rule by virtue of engaging in such activities. Accordingly, investments by U.S. persons to subscribe for our H Shares in the [REDACTED] would constitute covered transactions subject to the notification requirements under the Final Rule. Any such notification obligation would apply to the relevant U.S. persons subject to the Final Rule (and not to our Company or any other parties involved in the [REDACTED]) and would require notification to the U.S. Department of the Treasury.

A U.S. person is required to conduct a reasonable and diligent inquiry to assess whether it has any compliance obligations under the Final Rule. Where a U.S. person is required to report a notifiable transaction, it must electronically submit a notification to the U.S. Treasury within 30 calendar days following completion of the transaction. The notification must include the information specified in § 850.405 of the Final Rule, together with the certification required under § 850.203.

Following the [REDACTED], U.S. persons may invest in our publicly traded Shares without being required to comply with the above notification requirements, as such investment would be exempted, to the extent that they are not afforded any rights in the Company beyond standard minority shareholder protections.