CHINA
REGULATORY UPDATES

瀚一律师事务所
HAN YI LAW OFFICES

www.hanyilaw.com

August & September 2021

TABLE OF CONTENTS / 本期内容

CYBERSECURITY / 网络安全

Companies Seeking Overseas Listing Facing Stricter Cybersecurity Review 拟赴国外上市公司面临更严格网络安全监管

2021年7月10日，中国互联网信息办公室（“网信办”）发布《网络安全审查办法》（修订草案征求意见稿）（“草案”）。本次修订为《网络安全审查办法》自2020年6月生效以来的首次修订，在《数据安全法》于今年6月正式出台、网信办近期对滴滴等在美上市企业集中启动网络安全审查的背景下，本次修订备受社会关注。相比2020年《网络安全审查办法》，草案有如下要点：

1. 特定拟国外上市公司须进行网络安全审查申报：修订草案提出了“掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”并提交寻求国外上市的“IPO资料”的要求，中国证监会也同时被列入国家网络安全审查单位。此调整是继2021年7月6日《关于依法从严打击证券违法活动的意见》出台后，国家对拟国外上市公司数据安全、数据跨境传输、数据信息披露等方面监管的有力落实。草案也提出了一些系列问题，其中，“国外上市”是否包括在香港上市引发了较大的讨论。与以往的“境外上市”不同，草案采取“国外上市”的表述可能有意将拟在香港上市的企业排除在申报义务人的范围以外。草案同时也提出了一系列问题，如“IPO材料”的定义与范围，草案对已外国上市公司是否有溯及力等，这些问题有待未来实施细则与实践进一步明确。
2. 衔接数据安全法：草案将数据处理者纳入网络安全审查的义务主体，并将数据处理活动纳入到网络安全审查的范围，同时相应增加了《数据安全法》作为立法依据。这是在网络安全框架下对《数据安全法》中现有的数据安全审查制度的落地，也是对关键信息基础设施运营者所掌握的核心数据、重要数据及个人信息的进一步保护。

On July 10, 2021, the Cyberspace Administration of China (“CAC”) released the Cybersecurity Review Measures (Revised Draft for Public Comments) (the “Draft”). This Draft is the first revision since the Cybersecurity Review Measures took effect in June 2020. With the Data Security Law being formally introduced in June this year and the recent cybersecurity reviews of several U.S.-listed PRC companies (such as Didi) launched by CAC, the Draft has provoked widespread discussions. Compared with the 2020 Cybersecurity Review Measures, highlights of the Draft include, among others:

1. **Certain companies seeking to list in foreign countries are required to report for cybersecurity review**. The Draft provides that operators holding personal information of more than 1 million users must report for cybersecurity review with the Cybersecurity Review Office when seeking to list in a foreign country and are required to submit, *among other things*, the “IPO materials”. Notably, the China Securities Regulatory Commission or CSRC is also listed as one of the national cybersecurity review authorities. Following the introduction of the “Opinions on Lawfully and Strictly Combating Illegal Securities Activities” on July 6, 2021, this Draft signals a strong implementation of data security supervision, cross-border data transmission control and data disclosure requirements for companies proposed to list in other nations. The Draft also raises a series of questions, such as whether “listing in a foreign country” will include listing on the Hong Kong Stock Exchange. By using the expression of listing in a “foreign country” rather than “offshore listing” (a phrase which has been commonly used before), the Draft may intend to exclude companies to be listed or already listed in Hong Kong from the reporting obligations. Other questions include the definition and scope of “IPO materials” and whether the Draft will apply retroactively to companies already listed in foreign countries, etc. These questions remain to be further clarified by future legislations and practice.
2. **Compliance with the Data Security Law**. The Draft adds the Data Security Law as one of its legislative basis, while obligating data processors for cybersecurity review and including data processing activities into the scope of cybersecurity review accordingly. This is the reflection of the existing data security review system under the Data Security Law and is also a further protection of core data, important data and personal information held by critical information infrastructure operators (“CIIOs”).

China Passed Personal Information Protection Law 《个人信息保护法》颁布

2021年8月20日，全国人大常务委员会审议通过《个人信息保护法》（“《保护法》”），将自2021年11月1日起施行。在《网络安全法》《数据安全法》等现有法律的基础之上，《保护法》进一步明确及完善了个人信息处理及保护规则，主要有以下方面值得关注：

1. 扩大个人信息的范围：《网络安全法》及《民法典》等现有法律对个人信息进行了基本相同的定义，即“是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息”，其核心在于能够“识别”特定自然人。《保护法》将进一步将个人信息定义为“以电子

On August 20, 2021, the National People’s Congress Standing Committee passed the PRC Personal Information Protection Law (the “PIPL”), which will take effect on November 1, 2021. Building on top of the Cybersecurity Law and Data Security Law, the PIPL enhances the personal data protection and clarifies personal data protection principles. Highlights of the PIPL include:

1. **Expanding the scope of personal information**. According to the Cybersecurity Law and the PRC Civil Code, “personal information” means “various information recorded electronically or in other ways that can identify the personal identity of a natural person when using alone or in combination with other information”. The gist of this definition is the ability to “identify” a natural person. The PIPL further defines “personal information” as “any information recorded electronically or by otherwise means,

或者其他方式记录的与已识别或者可识别的自然人有关的各种信息……”，即除了能够“识别”自然人的信息外，还包括与该自然人“有关”的信息，一定程度上扩大了现有法律规定的个人信息的范围。《保护法》对于个人信息的上述定义与欧盟《通用数据保护条例》（GDPR）对于个人信息的定义较为相似，并且体现了我国个人信息保护领域的重要国家标准《信息安全技术 个人信息安全规范（GB/T 35273-2020）》（2020年10月起实施）提出的个人信息判定规则，即应考虑两条路径：“一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息即为个人信息”。

2. **明确域外适用情形**：《网络安全法》未明确规定其具有域外效力，《数据安全法》也仅原则性规定在中国境外开展数据处理活动，损害中国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。而《保护法》则借鉴了GDPR等境外法律对于域外效力的规定，明确了在境外处理中国境内个人信息的活动应适用《保护法》监管的三种情形：(i)以向境内自然人提供产品或者服务为目的；(ii)分析、评估境内自然人的行为；(iii)法律、行政法规规定的其他情形。此外，《保护法》还要求相关境外处理者应当在中国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将联系方式等报送主管机关。因此，对于一些业务经营地在境外、但主要客户为境内个人的互联网平台，应注意加强对于个人信息保护境内合规风险的评估及整改。

3. **完善个人信息跨境提供规则**：《网络安全法》及《数据安全法》仅原则性规定了关键信息基础设施运营者（CIIO）跨境提供个人信息的规则，而《保护法》则以专门章节具体规定了个人信息跨境提供的规则：(i)首先，个人信息处理者向境外提供个人信息应当通过以下路径之一：通过国家网信部门组织的安全评估、经专业机构进行个人信息保护认证、按照国家网信部门制定的标准合同与境外接收方订立合同、或者按照中国缔结或参加的国际条约和协定等向境外提供个人信息；(ii)其次，个人信息处理者跨境提供个人信息时应当(a) 采取必要措施，保障境外接收方处理个人信息的活动达到《保护法》规定的个人信息保护标准；(b) 向个人告知境外接收方的姓名、联系方式等，并取得个人的单独同意；以及(c)事前进行个人信息保护影响评估；(iii)特别地，在《网络安全法》规定的CIIO收集和产生的个人信息和重要数据应当在境内存储、向境外提供应通过国家网信部门组织的安全评估的基础之上，《保护法》新增了“处理个人信息达到国家网信部门规定数量的个人信息处理者”应当与CIIO同样受限于该等要求。该条所提及的“规定数量”有待国家网信部门进一步明确。

此外，在法律责任方面，《保护法》规定了警告、一百万元以下罚款、没收违法所得、停业整顿等处罚措施。总体而言，《保护法》对个人信息保护相关问题

which are related to an identified or identifiable natural person”. The key factor under the PIPL to determine whether certain information is personal information is not only whether such information is able to identify a natural person, but also whether it is related to such natural person. Similar to the definition of personal information in the EU's General Data Protection Regulation (GDPR), this definition of personal information under the PIPL also reflects the test for determining personal information under the “Information Security Technology Personal Information Security Specification” (GB)/T 35273-2020)" (implemented in October 2020), which includes two paths: “the first is identification, that is, from information to individual. Identifying a particular person by a particular information. The second is association, that is, from individual to information. Any information generated by a particular person in his/her activities is personal information.”

2. **Extraterritorial jurisdiction**. The Cyber Security Law does not clearly stipulate that it has extraterritorial jurisdiction, and the Data Security Law only stipulates in principle that data processing activities conducted outside the PRC that may “harm the national security or public interests of the PRC, or the legitimate rights of Chinese citizens or entities” will be punished. The PIPL, however draws on the provisions of the GDPR and other foreign laws and clarifies that the following activities, albeit conducted overseas, shall still be subject to the jurisdiction of PIPL: (i) with the purpose to provide a product or service to domestic individuals; (ii) to analyze or assess the behavior of domestic individuals; or (iii) any other circumstance as provided by law or administrative regulations. Additionally, the PIPL also requires relevant overseas data processors to establish specialized agencies or designate representatives in China to handle personal information protection related matters, and to submit contact information to competent authorities. As a result, internet platform companies whose business operations are abroad but whose main customers are PRC domestic individuals should pay special attention to the personal information protection compliance risks and corresponding rectification measures.

3. **Improving rules for cross-border provision of personal information**. Both Cybersecurity Law and Data Security Law only generally stipulate rules for cross-border provision of personal information by critical information infrastructure operators or CIIOs, yet the PIPL specifies in a special chapter rule for cross-border provision of personal information. Pursuant to the PIPL, (i) personal information processors shall provide personal information abroad through one of the following paths: passed the security assessment organized by the State cybersecurity and informatization department, certified by professional institutions regarding the personal information protection, enter into contracts with overseas recipients in accordance with the standard contract formulated by the State cybersecurity and informatization department or provide personal information abroad in accordance with international treaties and agreements acceded to by China. (ii) Second, when personal information processors provide personal information across borders, they should (a) take necessary measures to ensure that the activities of overseas recipients in processing personal information will meet the personal information protection standards specified in the PIPL; (b) notify the individual about the overseas recipients’ name, contact information, handling purpose and methods etc., and obtain separate consent from the individual; and (c) conduct prior impact assessment of personal information protection; (iii) particularly, in addition to the requirements that personal information and important data collected and generated by CIIO should be stored domestically and shall pass the security assessment by the State cybersecurity and informatization department before providing abroad, the PIPL also requires that "personal information processor processing personal information up to certain amount as prescribed by the State cybersecurity and informatization department " shall also be subject to the above

进行了较为详细的规定，与已经颁布的《网络安全法》、《数据安全法》等法律共同搭建我国数据安全的法律框架，有利于更好地保护个人信息权益、规范个人信息处理活动，以及促进个人信息合理利用。

requirements. The "certain amount" remains to be further clarified by State cybersecurity and informatization department.

Separately, in terms of legal liabilities, the PIPL stipulates penalties such as warnings, fines of less than RMB 1 million, confiscation of illegal income, and suspension of business. The PIPL generally provides more detailed regulations on personal information protection related matters, and works in concert with the Cyber Security Law, Data Security Law and other laws to build the PRC legal framework for data security, providing enhanced personal information protections and more obligations on personal data processors to promote the rational use of personal information.

State Council Passed Regulations on Security Protection of Critical Information Infrastructure 国务院发布《关键信息基础设施安全保护条例》

2021年7月30日，国务院发布《关键信息基础设施安全保护条例》（“《条例》”），《条例》将于2021年9月1日生效。《条例》在《网络安全法》的基础上，就关键信息基础设施（“CII”）的认定、运营者（“CIIO”）的责任义务、CII保障和促进措施等方面进行规定。其中，有以下几个问题值得关注：

1. **CII的认定规则由保护工作部门制定**：《网络安全法》规定，CII的具体范围和安全保护办法由国务院制定。《条例》进一步规定，CII认定规则由保护工作部门，即CII涉及的重要行业和领域的主管部门和监督管理部门制定。也就是说，不同行业、领域的CII认定规则，有待相应行业、领域的保护工部门出台更加具体的文件予以明确。同时，在CII涉及的行业和领域方面，与《网络安全法》相比，《条例》新增了“国防科技工业”这一表述，并明确优先保障能源、电信等CII安全运行。在制定CII认定规则时，《条例》规定需要考虑对关键核心业务的重要程度、遭到破坏时可能带来的危害程度，以及对其他行业和领域的关联性影响。

2. **CIIO的主要负责人负总责**：关于CIIO的责任义务，《条例》明确，CIIO的主要负责人对CII安全保护负总责，领导CII安全保护等工作。总的来看，《条例》沿用了《网络安全法》中的部分规定（例如，CIIO应当设置专门安全管理机构），并新增了一些内容（例如，规定了专门安全管理机构的具体职责）。

3. **军队参与保护CII安全**：在CII的保障和促进措施方面，《条例》新增由军队和地方政府协同保护CII安全的规定。另外，《条例》规定由保护工作部门制定具体行业、领域的CII安全规划，以明确工作任务和具体措施等。

除上述内容外，由于《条例》细化了CIIO的责任义务，因此也相对更细致地规定了违反相应责任义务时CIIO的法律责任，包括警告、一百万元以下罚款等。总体而言，《条例》围绕CII相关的核心问题进行规定，为CII的认定、保护等提供了一定的可操作性，有利于进一步保障CII安全，维护网络安全。

On July 30, 2021, China’s State Council passed the Regulations on the Security Protection of Critical Information Infrastructure (the “Regulations”), which will take effect on September 1, 2021. Based on the PRC Cybersecurity Law, the Regulations stipulate key issues such as the identification of critical information infrastructure (the “CII”), the responsibilities and obligations of the CII operators (the “CIIO”), and the measures on the protection and advancement of the CII, etc. Highlights of the Regulations include:

1. **Rules for identification of the CII to be formulated by the security protection departments**. The PRC Cybersecurity Law has provided that the specific scope and measures for security protection of the CII shall be formulated by the State Council. The Regulations further clarify that the CII identification rules shall be formulated by “security protection departments”, which means competent authorities in important industry and fields. That is to say, different industries and fields may implement different set of rules to identify CII. Additionally, in terms of the industries and fields involved in CII, compared with the Cybersecurity Law, the Regulations added “National Defense Technology Industry”, and explicitly prioritizes the safe operation of CII in the fields of energy and telecommunications. When formulating its identification rules, the Regulations stipulate that it is necessary to consider the CII’s importance to the core business, the potential harm it may cause when damaged, and the chain reaction to other industries and fields.

2. **The principal of the CIIO to take the overall responsibility**. Regarding the responsibilities and obligations of CIIO, the Regulations clarify that the main person in charge of CIIO is responsible for CII security protection and leads CII security protection work. In general, the Regulations follow some of the provisions of the Cyber Security Law (for example, CIIO should set up a special security management agency), and add some new content (for example, specify the responsibilities of the special security management agency).

3. **The military’s cooperation in protection of the CII**. In terms of CII safeguards and advancement measures, the Regulations have added the military to coordinate with local governments to protect CII. In addition, the Regulations stipulate that the protection work department shall formulate CII safety plans for specific industries and fields.

In addition to the above, as the Regulations detailed CIIO's responsibilities, it also specified the corresponding legal consequences of CIIO in a more detailed manner, including warnings, fines of less than one million yuan, etc. In general, the Regulations stipulated the core issues related to CII, provided guidance for the identification and protection of CII, and is helpful to further enhance CII security and network security.

EDUCATION / 教育

China to Overhaul Curriculum-Related Private Education Outside of School System 中国将整顿学科类校外培训行业

7月24日，中共中央办公厅、国务院办公厅印发《关于进一步减轻义务教育阶段学生作业负担和校外培训负担的意见》（“意见”），针对长期以来校外培训行业存在的总数过大、资本化运作、违法违规情况突出等问题进行了集中整治。具体来说：

1. **从严审批机构**：对于学科类校外培训，意见要求各地不再审批新的面向义务教育阶段学生的学科类校外培训机构，现有学科类校外培训机构重新审核并统一登记为非营利性机构，原已备案的线上学科类校外培训机构须重新办理审批手续。对于非学科类培训机构也将由各主管部门分类制定标准严格审批。
2. **禁止学科类培训机构资本化运作、禁止引入外资**：意见明确禁止学科类培训机构上市融资，要求上市公司不得通过股票市场融资投资学科类培训机构，不得通过发行股份或支付现金等方式购买学科类培训机构资产；外资不得通过兼并收购、受托经营、加盟连锁、利用可变利益实体等方式控股或参股学科类培训机构。

此外，意见还在培训机构课时、学生作业量、学校课后服务、教育质量等多方面提出了进一步要求，以推动教育回归公益本质，减轻学生家长负担。意见出台后，北京等试点城市已陆续出台细则，我们也将持续进行关注。

On July 24, the General Office of the CPC Central Committee and the General Office of the State Council issued the *Opinions on Further Reducing the Burden of Homework and Off-Campus Training for Students at the Compulsory Education Stage* (the “Opinions”), which focused on the long-standing problems of excessive total amounts of off-campus training institutions, capitalized operations, and violations of laws and regulations in the off-campus training industry. Highlights of the Opinions include:

1. **Strict approval of institutions**: For curriculum-related off-campus training, the Opinions require that no new institutions should be approved, existing curriculum-related off-campus training institutions should be re-examined and uniformly registered as non-profit institutions, and formerly registered online curriculum-related off-campus training institutions should be subject to re-approval procedures. Non-curriculum-related off-campus training institutions will also be subject to strict examination and approval by competent authorities.
2. **Prohibit the capitalization of curriculum-related training institutions and the introduction of foreign capital**: the Opinions specifically prohibit the listing of curriculum-related training institutions for financing, requiring listed companies not to invest in curriculum-related training institutions through stock market financing, and not to purchase the assets of curriculum-related training institutions by issuing shares or paying cash; foreign investors shall not control or hold shares in curriculum-related training institutions through mergers and acquisitions, entrusted operations, franchise chains, and the use of variable interest entities.

In addition, the Opinions also raise further requirements in such aspects as the hours of training institutions, homework amount for students, school’s after-class services, and the quality of education, in an effort to promote education to return to the essence of public welfare and reduce the burden on students and parents. After the introduction of the Opinions, Beijing and other pilot cities have issued local rules, and we will continue to monitor further developments in this area.

For further information, please write us at ***inquiry@hanyilaw.com.***

CONTACT US

上海市中山西路2020号
华宜大厦1座1801室
邮编：200235
电话：(86-21) 6083-9800

Suite 1801, Tower I, Huayi Plaza
2020 West Zhongshan Road
Shanghai 200235, China
Tel: (86-21) 6083-9800