Higher-Ed's New GDPR: What Your Institution Needs to Know About PIPL

Higher education institutions have become all too familiar with the extraterritorial approach of international privacy laws. When the European Union's General Data Protection Regulation (GDPR) went into effect in 2018, higher education institutions were heavily impacted, and had to quickly adjust and implement various compliance mechanisms. Just when the dust has settled on GDPR, China passed its own comprehensive privacy law, the Personal Information Protection Law (PIPL). These institutions should take note on PIPL's applicability and certain steps to comply with this new law. For additional background information on PIPL, please visit our previous post summarizing the new law before it went into effect.

How does PIPL apply to higher education institutions?

PIPL went into effect recently, on Nov. 1, 2021. Like GDPR, PIPL is a national law with extraterritorial scope, meaning it applies to entities doing business both within and outside of China that process personal information on natural persons within the territory of China. PIPL's objectives are to protect the rights and interests of individuals, regulate personal information processing activities and facilitate reasonable use of personal information. Higher educational institutions may be subject to PIPL if they process personal information of Chinese residents for the purposes of (i) providing products or services to individuals in China, (ii) "analyzing" or "assessing" the behavior of individuals in China, or (iii) as provided in Article 3 of PIPL, for other purposes to be specified by laws and regulations. As a result, any higher education institution that, for example, obtain admissions' applications from Chinese citizens while the individual is located in China, conduct recruitment in China, respond to requests for information from individuals located in China, conduct research using data from Chinese citizens (that is not anonymized) or work with Chinese academic institutions or organization, may potentially be implicated by PIPL.

What is the definition of personal information?

The law defines "personal information" broadly as all information related to identified or identifiable natural persons, but makes it clear that anonymized data does not trigger PIPL. Like GDPR, there are also sensitive information categories that requires additional safeguards, which may include information on medical, financial or location information. When processing this type of data, higher educational institutions will likely be required to obtain an individual's informed consent.

Does PIPL require lawful basis for processing?

Yes, like GDPR, PIPL requires institutions to justify their data processing via certain enumerated lawful bases. However, unlike GDPR, PIPL does not provide a "legitimate interest" catchall as a lawful basis for processing personal data. Overall, PIPL appears to be a more consent driven regulation than GDPR and requires individual and specific informed consent for numerous processing activities. PIPL's definition of consent is very similar to GDPR, and requires the consent to be informed, freely given, demonstrated by a clear action of the individual and must be allowed to be withdrawn.

Are there fines for noncompliance with PIPL?

PIPL includes substantial fines for noncompliance. Failure to comply with this law could potentially result in steep fines of over $7 million or up to 5% of your organization's annual revenue of the previous fiscal year. PIPL does contemplate individual liability. Further, like GDPR, there is a private right of action for individuals. Therefore, if your higher educational institution processes data of individuals located in China, taking critical steps to comply with PIPL is essential.

Has there been any further information about PIPL since it went into effect?

There are still many unanswered questions about PIPL that will be answered in the coming months and years. However, looking to other laws in China may give some guidance on PIPL compliance. PIPL is the newest law surrounding the regulation of personal information, but it will likely function in collaboration with portions of two other existing laws, the Cybersecurity Law (CSL) (effective since 2017) and the Data Security Law (DSL) (effective since Sept. 2021). At the end of November, the Cyberspace Administration of China (CAS) published draft regulations for public comment on Network Data Security Management. Once effective, the draft regulations will impose even greater compliance obligations on PIPL covered entities, including strict data beach reporting obligations, record retention obligations and compliance reporting.

What action(s) should your organization take?

Although there are still unanswered questions concerning PIPL, there are a number of steps that higher education institutions can take towards compliance. This includes, as a first step, identifying students who may be affected as a result of this new law. In addition, institutions should update their public-facing privacy policies to include the necessary disclosures under PIPL, as well as update internal policies and procedures concerning consumer requests, secure transfer and processing, etc., as well as update their vendor contracts. Lastly, because consent is imperative to compliance with PIPL, institutions should develop consent mechanisms and implement them as soon as possible.

For more information regarding China's Personal Information Protection Law and to discuss compliance efforts businesses should be taking, contact Amber Lawyer, CIPP/E, Shannon Knapp, CIPP/US or any attorney the Cybersecurity and Data Privacy practice.

Thank you to Associate Trainee Hoda Moussa for her help drafting this information memo.

BOND SCHOENECK & KING ATTORNEYS