China Data Protection

The National People's Congress (NPC) of China adopted on August 20, 2021 the first Chinese comprehensive data protection law, the Personal Information Protection Law (PIPL), less than a year after the first draft of the law was published. The NPC thus concluded its legislative process that saw two additional markups of the law since October of last year. The PIPL will go into effect on November 1, 2021, but many companies within China are already coordinating with relevant enforcement agencies to comply.

The PIPL should not affect Anteriad but tread with caution when receiving Chinese data as the 'handler' can also be accountable if the Chinese Company is not compliant – China is predominantly using this Law to target Tech companies such as online platforms who hold a lot of personal information/geo location etc. Ensure Data Transfer Agreements are signed (this should be given to the 'Handler') plus ensure due diligence is meticulously carried out. Use Opted In Data at all times.

- There is no distinction between B2C & B2B
- China have adopted GDPR model but with added twists
- Predominantly Consent Driven, like GDPR, however, under their 7 Legal Bases, there is no Legitimate Interest, but this could change before official enactment date
- The Law is applicable to Chinese Companies only, however, it can affect the US as a data 'handlers' – if the Chinese company is not compliant, they can immediately be closed down, but receivers are also in the frame for legal action
- Targeting Tech Companies - This applies to companies that are "foundational internet platforms", have a large number of users, or have complex operational models. While it is not exactly clear as to what types of companies the PIPL applies to, its provisions appear to target internet, social media, and artificial intelligence giants like Alibaba, Baidu, and Tencent – all of whom handle vast amounts of private information.
- The PIPL represents one pillar of China's emerging data protection architecture that includes a myriad of other laws, industry-specific regulations, and standards. For instance, the recently enacted Data Security Law (DSL) sets forth a comprehensive list of requirements regarding the security and transferability of other types of data. It also establishes a "marketplace for data" to enable data exchange and digitalization. Additionally, the PIPL explicitly references China's Constitution to provide a firmer legal basis for the implementation of its data protection goals! The PIPL should not be viewed in isolation but examined in relation to other regulatory Laws.
- The PIPL has several other objectives, which distinguishes it from the majority of data protection laws globally. The law has a distinct 'national security' flavor, particularly around cross-border transfers. It incorporates provisions that affirm China's intention to defend its digital sovereignty: overseas entities which infringe on the rights of Chinese citizens or jeopardize the national security or public interests of China will be placed on a blacklist and any transfers of personal information of Chinese citizens to these entities will be restricted or even barred. China will also reciprocate against countries or regions that take "discriminatory, prohibitive or restrictive measures against China in respect of the protection of personal information"
- Its 'officially' declared aims are:
    - to protect the rights and interests of individuals
    - to regulate personal information processing activities
    - to safeguard the lawful and "orderly flow" of data
    - to facilitate reasonable use of personal information