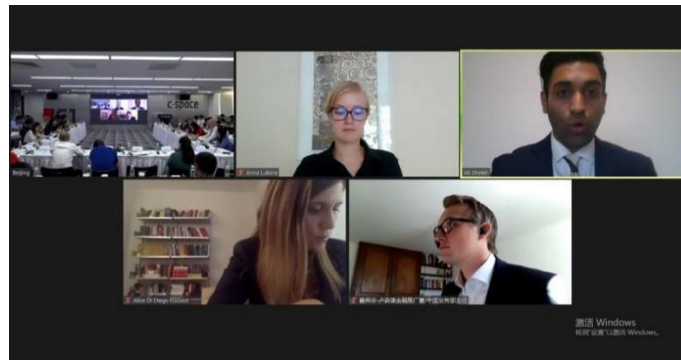




Cross-Border E-commerce – Legal Issues to Consider

On September 8th, Ms. Anna Lukina, Director of Business Development and Marketing at the European-American Desk of A&Z Law Firm, spoke at the 'International Seminar on Digital Trade & Innovation Resources Partnership'. Both offline and online event, it brought together experts from different fields, all united by their involvement in the development of digital trade. Organized by the Beijing Municipal Bureau of Economy and Information Technology, as well as 761C Space in Beijing, it was an afternoon of presentations and panel discussions.



Ms. Lukina participated in an international panel, together with Mr. Rafael Jimenez Buendia, Mr. Ali Sheikh, Mr. Chris Hollifield and Ms. Alice Di Diego, all esteemed professionals, who each brought a different perspective on digital trade and the vast opportunities it creates. On behalf of A&Z Law, Ms. Lukina shared some of the legal issues that cross-border E-commerce ('CBEC') businesses frequently face, stressing that with an increasing number of regulations, compliance is essential for companies all over the world.



CROSS BORDER E-COMMERCE

LEGAL ISSUES TO CONSIDER

September 8, 2020

At A&Z, we assist businesses to reach their full potential, by helping them to understand the legal hurdles they may be facing during their operations and growth. In her speech, Ms. Lukina presented and analysed two scenarios, and explained some of the most recent or pressing legal issues for CBEC in each one: first, for **companies entering Europe**, and subsequently for those **entering China**.

CBEC Legal Issues - When Entering Europe

General Data Protection Regulation

The long-awaited European Union ('EU') General Data Protection Regulation ('GDPR') entered into force on May 25th, 2018, becoming the most severe personal data privacy regime in the world. The regulation imposes strict rules on the collection, use and storage of personal data, which includes one's national ID number, address, bank information and more.

The national data protection authorities are responsible for the enforcement of GDPR, and they do it through investigations and audits of companies. This implies that Chinese companies who fail to defend an EU Member State enforcement action could be subject to a default judgment and all this entails. GDPR is the first EU regulation on data privacy and is automatically applicable in all 28 EU Member States.

As to the relevance for Chinese businesses, GDPR applies to the processing of personal data of people who are in the EU. Whenever either offering goods or services, regardless of whether a payment is required or monitoring people's behaviour in the EU. As a consequence, companies that offer products

and services to individuals in the EU via their websites or other online platforms now have to comply with EU data protection rules. Even if an e-commerce Chinese company does not have any formal establishments in the EU, GDPR will nonetheless apply in relation to these two types of activities.

GDPR applies to all databases, marketing, sales, HR and accounting. Our advice is to start by comparing the GDPR requirements with your current measures.

Here is a non-exhaustive checklist of things you need to do to ensure you comply with GDPR:

- Decide what data from the EU you need to store and confirm you have the correct permissions
- Ensure all the third-party applications used to support the storage of data comply with the GDPR
- Revise the site's privacy policy and/or disclosures to comply with GDPR
- Determine whether the company needs to appoint a Data Protection Officer
- Make consent clear and actionable, as mandated by the GDPR

CE Marking and Quality Compliance

CE marking is not a product standard, but a conformity mark signalling compliance, specifically, with all applicable European Economic Area directives. The directives and technical standards, change depending on the product type. As each directive regulates specific products, their scope of regulation varies. Some directives regulate substances, while others regulate energy efficiency and electrical safety. Product compliance requires more than a printed CE mark. You must ensure that the items comply with all technical standards and requirements- Importing and selling non-compliant items in the EU is illegal, and may result in both a forced recall and major fines.

CE marking is required if you are either importing or exporting to an EU member state. As a result, CE compliance is therefore critical for both EU-based companies importing goods, and exporters selling to the EU – either as traditional B2B exporters or B2C CBEC sellers.

In a nutshell, in the past the EU saw an influx of non-compliant and unsafe products, originating from CBEC companies. As a result, now all requirements of the CE marking directives apply to the manufacturer irrespective of their location in the world. Chinese manufacturers must fulfil the obligations of the CE directives if they have the intention of making their products available in the EU.

CBEC Legal Issues - When Entering China

Cyber Security Law

An example worth highlighting is the Cyber Security Law ('CSL'), and there are several reasons why it has had a huge impact on CBEC. CSL has been in effect from June 1st, 2017, has for the first time introduced a framework for comprehensive regulation, regarding the privacy of electronically stored data in China. CSL includes a set of data protection provisions, in the form of national-level legislation. In other words, it is a law applied to all personal data, collected on information networks. It is designed to protect China from threats related to hacking, terrorism and other crimes.

It has had a significant impact on international businesses, notably because it also imposes some rules on companies based outside China, requiring them to store user information and other business-related data on servers located in China. It also requires firms to pass national security reviews and possibly share technological information with China's national security bodies.

Overall, organisations that operate in China, either domestically or internationally, should take a closer look at CSL, to ensure that the company's current practise is in line with the regulatory requirements.

Here is a non-exhaustive checklist:

- Take note of how information is collected, processed and stored, including private sensitive information
- Assess cybersecurity and privacy risks and threats in order to focus cybersecurity efforts on the most critical risks and threats.
- Set up a security and privacy incident monitoring system and appropriate reporting mechanisms
- Ensure proper safeguards of private and important information transmitted outside of China's borders
- Design a proper security incident response plan and perform periodic drills

E-commerce Law

Under the new E-Commerce Law, which came into effect on January 1st, 2019, e-commerce operators are required to delete users' personal data if they cancel their account (unless the terms and conditions of the site allow retention for a longer period). In addition, e-commerce providers must also implement specific technical measures to ensure security and normal operations, to respond effectively to cyber-incidents. They must prepare an emergency response plan to manage incidents, and report them

to the authorities.

Are foreign businesses subject to China's e-commerce law? It depends, because e-commerce law applies only to e-commerce businesses with activities within China, namely, registering as an e-commerce business entity in China. This means the possession of a Chinese business license is required to qualify as an e-commerce business operator.

Cross-border E-commerce Pilot Zones

On May 6th, 2020, China's State Council issued the *Approval of the Establishment of Integrated Pilot Zones for Cross-border E-commerce* in 46 cities and areas. According to the document, 46 cities will build new CBEC pilot zones, bringing the total number of such zones in China to 105. The new pilot zones will be constructed based on the experience related to the existing pilot zones, and will promote the development of the CBEC industry. Of course, this decision comes amid the COVID-19 outbreak, and aims to stabilize and encourage foreign trade and foreign investment. Companies can enjoy favourable tax policies, such as exemption of value-added tax and consumption tax on retail exports, and reduction of corporate income tax rates in the CBEC pilot zones.



In summary, CBEC most certainly has a bright future and will offer many opportunities in the years to come. But because of its rapid growth and evolution, countries around the world are increasingly regulating all forms of digital exchanges and trade.

More and more companies doing CBEC are in need of legal counsel, in order to seek advice and thus avoid unnecessary litigation scenarios. A&Z attorneys across 11 legal practices, including logistics,

labour and compliance, dispute resolution and other legal expertise are at your disposal to discuss your business needs and provide you with efficient and solution-oriented services.

