ISF

# THE CHANGING DATA PROTECTION AND PRIVACY LEGISLATION IN CHINA

## The impact on global Trade

On the 1st of September 2021 the Data Security Law came into effect in the People's Republic of China, which provided a national framework for information security and data protection. However, recent legislative developments have seen a shift in momentum and a focus towards protecting citizens' and state data, with the long-awaited Personal Information Protection Law being signed on the 20th of August 2021, coming into effect on the 1st of November 2021.

With less that three months to prepare, Chinese and non-domestic organisations have a significant task on their hands to become compliant. With the threat of administrative fines for non-compliance of 5% of annual turnover and even personal fines for responsible individuals of up to $154,000, the stakes have certainly increased. In order to make this journey to compliance as smooth and cost-effective as possible, the ISF's tools, methodologies, frameworks and reports can provide organisations with the help they need.

### What are the key changes?

Many commentators have called the Personal Information Protection Law the 'Chinese GDPR' as many of the requirements mirror the European regulation. With domestic and extra territorial implications, Chinese and international organisations, with either locations in China or those that process Chinese citizens data, must be compliant.

For example, some of the main changes can be summarised in the following:

- Organisations must gather consent from individuals to process, store or sell their data.
- For cross-border data transfers, processors and handlers must pass a security assessment and undergo a personal information protection certification.
- Chinese citizens and state data must be protected by 'handlers', akin to 'controllers under the GDPR, e.g. increased data subject rights, control over data portability, etc.
- Data governance frameworks must be in place, e.g. having a data protection officer in place.
- Data breaches must be notified in a timely manner.
- Personal information stored within China should not be provided to foreign or law enforcements groups unless approval is given from the Chinese government authority.

### What short and long-term strategies can organisations take?

Much like the implementation of the EU's GDPR, Chinese and non-domestic organisations can take some proactive steps to meet the new requirements stipulated in the Data Security Law and Personal Information Protection Law. For example, organisations should:

- Seek legal counsel both internally in China and for organisations with operations in the region. A local Data Protection Officer should be appointed in China to help with implementing guidance.
- Update privacy and compliance policies.
- Identify, understand and classify the different types of data gathered, processed and shared within their organisation, considering data flows both domestically and internationally.
- Consent mechanisms need to be built into systems that gather information from individuals and third parties in the form of policies, contractual arrangements and agreements.
- Understand notification requirements during a data breach, e.g., who to notify and why.

## How can ISF materials help?

1. **ISF: General Data Protection Regulation – Implementation guide**

Many of the requirements in the new Chinese laws mirror the requirements in the EU GDPR. To assist our Member organisations the ISF developed a practical implementation guide for the GDPR, touching on how to get consent, how to develop an appropriate contract, how to develop breach notification processes, etc.

2. **ISF: Information Risk Assessment Methodology 2**

To become certified compliant with these laws all organisations must demonstrate that they have risk assessed projects, systems, assets and processes accordingly, understanding their threat environment and their overall level of risk. ISF Members use the Information Risk Assessment Methodology and tool to do this.

3. **ISF: Protecting the Crown Jewels and Mission Critical Assets**

The new Chinese laws specifically stipulate that organisations must have processes in place to identify and classify the types of data they are gathering, e.g., Chinese state data, important data and personal data. The ISF developed a full report and methodology for identifying and protecting these types of 'Crown Jewels,' which touch upon types of data to assess, governance frameworks, etc.

4. **ISF: Security Architecture – Navigating complexity**

The development of a secure architecture is of high priority for Chinese organisations, to ensure that they have a structure in place that is protected against cyber attacks and data loss, whilst meeting all of the requirements in the new laws. The ISF developed a full report on how to develop secure platforms inside your organisation to store and share core data.

## GET IN TOUCH IF YOU'D LIKE TO FIND OUT HOW THE ISF CAN SUPPORT YOU

**Dan Norman**
Senior Solutions Analyst
**PHONE**
+44 (0) 7825 679754
**EMAIL** daniel.norman@securityforum.org
**LINKEDIN** Find me on LinkedIn