FORTRA

FACT SHEET (Boldon James)

Chinese Cybersecurity Law (CCL)

Regulating the Handling of Personal and Important Chinese Information

The Chinese Cybersecurity Law (CCL) provides a legislative framework to regulate the Chinese digital landscape, including the appropriate handling of personal information and important data.

This wide-reaching legislation mandates that data originating in China must be stored there, unless specific criteria are met. Should the data need to be transferred overseas for processing, the processor or 'Network Operator' must first conduct a security self-assessment. If the data contains personal information, individual consent is required from the data subject first; they must also be notified of who the data recipient is, the purpose, scope, content, and country the recipient resides in.

Where transfers meet the following criteria, the CCL requires network operators to entrust a government agency to conduct the security assessment and review:

- Transfers of personal information of over 500,000 citizens;
- Transfers that exceed 1TB;
- Transfers of data on sensitive subjects such as nuclear facilities, chemical biology, national defence or military, public health, large-scale engineering projects, marine environments, and sensitive geographical information;
- Transfers of network security information
- concerning system vulnerabilities and security safeguards of CII operators;
- Transfers of data involving the provision of personal information or important data to overseas recipients by CII operators; and
- Other transfers that potentially affect national security and public interests, or transfers where the industry regulators or supervisory authorities require review.

There are 3 circumstances defined where data transfers are entirely prohibited:

- Where the data subject has not consented or when it may infringe upon their interests,
- Where the cross-border transfer poses security risks to the national political system, economy, science and technology, or national defence, or societal or public interest could be jeopardized; or,

CCL At A Glance

What Is The Chinese Cybersecurity Law (CCL)?

The CCL regulates Chinese data deemed to be personal or important, as well as the organisations which collect, store, transmit, exchange and process it

When Did The Legislation Come Into Force?

The cybersecurity legislation came into place in June 2017, with enforcement commencing across the following year. Deeper detail is available in the Information Security Technology – Personal Information Security Specification May 2018

Who Regulates CCL?

Cyberspace Administration of China (CAC)

What Are The Implications Of Non-Compliance?

There are significant fines for non-compliance with the law - potentially up to 1,000,000 RMB. Additionally businesses can be closed, or face forfeiting their licencing to trade

- In other circumstances where the Chinese government deems it necessary.

In addition to undergoing security assessments, network operators transferring personal information must also conduct security reviews of their cross-border transfers once a year at a minimum, and report the assessment to the respective industry regulatory or supervisory authority. Additional assessments are required should the data recipient change, the data recipient or cross-border data transfer suffers a significant "security incident" or if there are significant changes in the purpose, scope, volume, or type of data being transferred cross-border.

In alignment with the global trend of the protection of an individual's data, the CCL also regulates the handling and use of personal information as well as the rights afforded to the individual's control of it.

Organisations that collect or handle personal information must do so with the user's consent and in accordance with the Law, administrative regulations and user agreements. Departments with legal responsibilities for cybersecurity supervision must ensure that all personal information obtained remains confidential. Individuals have explicit rights to request access, correction or deletion of their personal information.

Deeper detail on the requirements are provided in the Information Security Technology – Personal Information Security Specification (the Specification), dated May 1st 2018. The Specification also provides a security policy template to assist organizations in adopting the CCL.

Appropriate classification of files is the first step to visibility and awareness of the critical data in your organization. Boldon James Classifier can protect against breaches with rules to prevent unauthorized dissemination of regulated information. Classifier can detect personal information in files and attachments suggesting or applying classification accordingly. These intuitive tools and comprehensive reporting simplify adherence to Chinese Cybersecurity Law.

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports compliance with Chinese Cybersecurity Law by:

- Meeting the need as specified in CCL article 21 to 'Adopt measures such as data classification, back-up of important data, and encryption'
- Apply visual markings and metadata to documents over a market-leading range of applications to clearly demarcate 'personal information' and 'important data'
- Set intelligent classification and handling rules to ensure that data originating in China is not exfiltrated without previously obtaining customer consent
- Mark information for expiry, to adhere to retention requirements
- Supporting downstream 3rd party controls such as Access Control and Rights Management Solutions
- Demonstrating compliance through a comprehensive reporting capability

Don't Delay Your Preparations

Though the CCL legislation does not preclude the ability of non-domestic companies to manage Chinese data, it is vital that companies who do so ensure that they comply with, and are able to demonstrate, their adherence to these comprehensive regulations. Boldon James Classifier is an important component on an organization's broad information governance program and is a key component in addressing CCL requirements today, and as they mature over time.

Visit boldonjames.com/ccl for more information on how data classification can protect your sensitive data.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.