

# DATA PROTECTION IN CHINA

## APPLIES TO

Any organization in the world processing personal data originating in China.

## Personal Data:

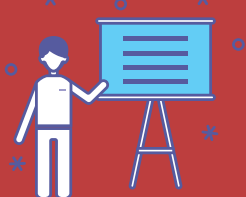
Any type of electronic information relating to an identified or identifiable person. (excluding anonymized data).

## RESPONSIBILITIES OF THE DATA PROTECTION OFFICER:

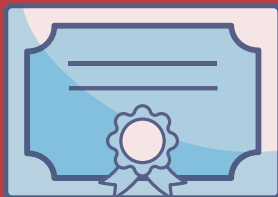
*Required for large organizations analyzing personal information of China.*



Ensure proper operation of **controls, rules, & security measures**



Conduct training & maintain records



Protection Impact Assessments & audits



Serve as contact for authorities + individuals

## Incident Response Obligations:

- \* Take corrective actions to mitigate harm of the incident.
- \* Inform affected individuals & authorities of the incident details.

## CONSEQUENCES OF VIOLATIONS:



Fines up to **¥50,000,000** or **5%** of global revenue for severe violations  
Up to **¥1,000,000** for **general** violations

Fines applied directly to the responsible **data protection officer(s)**:  
Up to **¥100,000**, or up to **¥1,000,000** for serious violations.

Risk of **class action lawsuits** from affected data subjects

Temporary or permanent **suspension of business**

## DATA TRANSFER REQUIREMENTS:

### DOMESTIC

- Establish **contractual measures** between controller and processor
  - **Inform** data subjects;
- Complete a Personal Information Impact Assessment (**PIIA**);
- **Limit** the personal data moved

### INTERNATIONAL

- Clear a CAC security evaluation  
**OR**  
Implement CAC standard contractual clauses with recipient
- AND**
- PIPL **compliant measures** set up;
  - Completion of a **PIIA**;
- **Separate explicit consent** from subjects & notice to them

**FOR MORE INFORMATION ON COMPLIANCE:**  
**US, EU & China's Data Protection Frameworks - Summarized**