eeCHECK

CHINA BACKGROUND CHECK PROCESS

Legal Framework & Employer Guide 2026

A comprehensive overview of employment screening
in Mainland China — PIPL • Cybersecurity Law • Data Security Law

Operational Complexity: High | Turnaround: 3–7 Business Days

LEGAL FRAMEWORK

Personal Information Protection Law (PIPL)

Regulates personal data collection, consent, purpose limitation, and cross-border transfers.

Cybersecurity Law

Governs data storage requirements, network security standards, and operator obligations.

Data Security Law

Oversees data classification, processing security, and national data security obligations.

Key Principles Employers Must Apply:

- **Explicit Consent**
- **Purpose Limitation**
- **Data Minimization**
- **Security Safeguards**
- **Clear Retention Controls**

CONSENT & CRIMINAL RECORD CHECKS

Consent Requirements

- Explicit written consent before any check
- Purpose-specific — state exactly why
- Transparent on data usage & retention
- Disclose cross-border transfers
- Name any third-party processors

Criminal Record Checks

Access	Strictly controlled
Application	Candidate must apply
Authority	Public Security Bureau (PSB)
Employer Use	Role-relevant & legally justified

⚠ *Always use official government channels only. Avoid unofficial databases.*

EMPLOYMENT & EDUCATION VERIFICATION

Employment Verification

Key Challenges:

– Company responsiveness variability

– Regional differences in record retention

– Corporate restructuring history

– Limited standardized HR documentation

Verification may include:

✓ HR department confirmation

✓ Supervisor confirmation

Education Verification

⚠ **Higher fraud risk vs. other Asian markets**

Checks include:

✓ Degree authenticity confirmation

✓ Institution accreditation validation

✓ Cross-check vs. official registries

Strongly recommended for:

Senior hires | **Technical roles** | **Executive positions**

RISK SENSITIVITY MATRIX

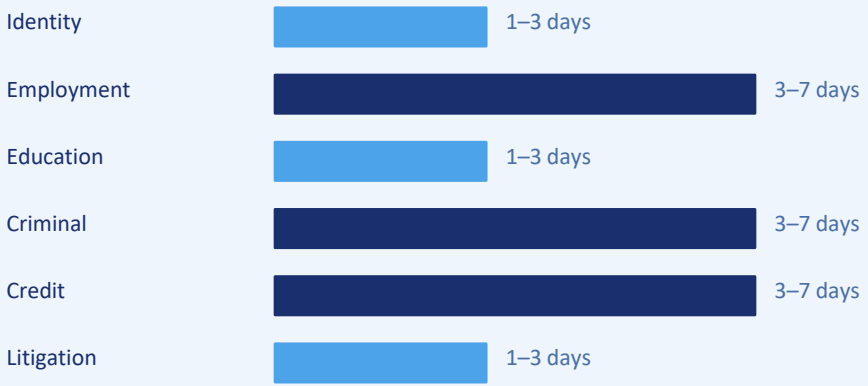
Check Type	Sensitivity Level	Legal Review
Identity	Moderate	No
Employment	Moderate	No
Education	Moderate	No
Criminal	High	Yes ✓
Credit	High	Yes ✓
Litigation & Financial Risk	Moderate–High	Yes ✓
Social Media	High	Yes ✓
Cross-Border Transfer	High	Yes ✓

DATA LOCALIZATION & TURNAROUND TIMES

Data Localization Risk

Data Localization:	May require in-country storage
Cross-border Transfer:	Security assessment may be needed
Sensitive Data:	High regulatory scrutiny
Large-scale Export:	Additional compliance obligations

Typical Turnaround Times



Common Mistakes to Avoid

- ✗ Ignoring cross-border rules
- ✗ Using unofficial data
- ✗ Over-collecting data
- ✗ Wrong consent format
- ✗ Assuming national uniformity

CREDIT & FINANCIAL CHECKS

Requirements

Explicit Consent
Candidate must give written consent before any credit data is accessed

Role-based Justification
Must demonstrate why financial data is proportionate to the role

Legal Permissibility
Review applicable laws before conducting; scope is restricted

Sensitive Data Handling
Subject to heightened controls under PIPL sensitive data rules

Clear Retention Limits
Define and document how long data will be held and who can access it

Most Relevant For:

- Senior Executives
- Finance & Treasury Roles
- Fiduciary Positions
- Regulated Industry Roles

Regulatory Caution

- China's credit reporting system (PBOC) is government-controlled
- Individual credit data access is heavily restricted by default
- Third-party credit bureaus operate under strict licensing
- Always obtain specialist legal advice before conducting credit checks

LITIGATION, RISK & VENDOR DUE DILIGENCE

Civil Litigation Search

Identifies court cases, legal disputes, and civil exposure history relevant to the candidate or entity.

Dishonesty List (失信人)

Identifies enforcement actions, court-ordered financial obligations, and blacklisted individuals.

Legal Representative Search

Reveals corporate involvement, directorship history, and potential conflicts of interest.

Proportionality Principles

01	Use only where relevant to the specific role and its risk exposure
02	Assess proportionality before collecting — document the business justification
03	Review findings carefully; do not make automatic adverse decisions
04	Engage legal counsel for candidates flagged on dishonesty lists

EXECUTIVE OVERSIGHT CHECKLIST

- [ ] **Is consent compliant with PIPL?**
  Written, explicit, purpose-specific consent required for all data processing
- [ ] **Is criminal verification via official channels?**
  Only Public Security Bureau (PSB) certificates accepted — no unofficial databases
- [ ] **Are cross-border transfers assessed?**
  Security assessments may be required for data leaving Mainland China
- [ ] **Is sensitive data classified properly?**
  Criminal, credit, and biometric data require heightened controls
- [ ] **Is screening scope role-proportionate?**
  Only collect what is necessary and justified for the specific position
- [ ] **Is documentation retained securely in China?**
  Data localization may mandate on-shore storage and access controls

COMPLIANCE IS NON-NEGOTIABLE

Screen Responsibly.

Protect Your Organisation.

China's regulatory environment demands jurisdiction-aware precision.

Explicit consent · Official channels · Data localization · Role-proportionate screening

For legal review and further guidance, consult qualified counsel familiar with PIPL, Cybersecurity Law, and Data Security Law.