5.3. Data Protection and Cybersecurity (RC)

Introduction

Data Protection and Cybersecurity have been a hot topic, even increasing more with the new cybersecurity law published in 2017. The new regulations bring more obligations for the IT infrastructure of network operators which includes any company that owns and manages a network. If your parent company is providing your IT infrastructure to a local entity which is set up to provide products and services in China, then they are to be considered as network operator and have to adhere to Chinese law.

The requirements can be structured into:

- Personal Information protection
- Data Transfer and
- Data Management/Governance.

Network operations security

All network operators have to ensure the security of their network, including

- Security management systems and operating policies
- Appointing a responsible person for data protection e.g. as a Data Protection Officer
- Use technical measures to secure the network against misuse, e.g. by running security software
- Monitor and record intrusions or unlawful activities
- Ensuring backups, access protection and encryption of classified data.

Personal Information Protection

Personal Information can be separated into

- personal information which is related to people but cannot be used to identify a specific person and
- personal identifiable information (PII) which can be used to identify a specific person.

The standards regulate how personal data can be collected, stored, handled and shared. Some critical points to consider:

- User consent of collected data is to be ensured and it must be made clear what the purpose of the data is
- Personal data collection without specific purpose is forbidden
- Sharing data with other entities can only be done if the person agreed to it or if it has been anonymized
- If personal information is being leaked or if it is likely that it was leaked, affected users have to be informed without delay and the relevant government authorities have to be informed
- If the data collection is unlawful or unauthorized, affected users can request the deletion of the data.

Data transfer

The unlawful transfer of data to third parties is forbidden. Do not forget to keep these topics in mind:

- Data may only be shared with other entities if the person agreed to it or if it has been anonymized
- Data transfer to other countries for Critical Information Infrastructures (CII) is only allowed if the data is stored in China first. This means that the data can only be copied to other countries. Other data can be transferred abroad directly as long as the user gave implicit or explicit consent and a security assessment has been done.
- If you are using external service providers for data collection, storage and handling, they should be properly audited, either by yourself or by an authorized third party institution or even a governmental certification.

Importance of Data Protection and privacy rights

Data Protection and privacy rights are stipulated in the General Provisions of the civil law in Article 110 and 111 which – amongst others - regulates that information security

must be ensured when collecting personal data and that this data must not be unlawfully disclosed to others, including selling the information.

Are you a Critical Information Infrastructure?

Data protection is highly integrated into a complete framework of rules and regulations which also addresses critical information infrastructures: These are defined as providers which could cause serious consequences if they suffer damage or lose their function. Since there are additional regulations concerning these, it is recommended to check article 31 of the Cybersecurity law yourself if you could be considered as one.
First hints to check for can be

- type of industry (e.g. nuclear, military, financial)
- data of a large number of persons
- data that can have a serious impact on public infrastructure (e.g. availability of water, heating and electricity).

If your company is classified as a CII company, additional requirements are being put in place, e.g. the execution of an annual security assessment, required security and confidentiality agreements with vendors, creation of emergency response plans, regular training and evaluation of personnel regarding cybersecurity or even the need for a yearly security review with authorities.

Your company website

If you want to provide a legally compliant website in China, you require an ICP license. It should be either stored locally on servers by a licensed provider in China or using compliant Content Distribution Services which can also dramatically increase the access speed.
Some certain functions, e.g. providing an online shop on your website yourself, can also be limited either by your business license or by local law.

Data Protection Healthcheck

One of the biggest challenges to check your compliance with regulations can be that you at first have a missing transparency what kind of data your company is actually using and how it is being processed.
For Analyzing if your current data infrastructure meets the requirements, I would recommend to first create a process map of your company and identify the critical processes in which personal or critical data is being used. My personal preferred form is creating a map which is similar to the porter value chain.
After you identified the relevant processes, a detailed list of the collected information, in which IT systems they are stored and which departments are working with them can be documented.
With a transparency like this, you will have it much easier to compare the current state to the requirements.

Quick Assessment

For a first quick assessment to at least prevent the biggest mistakes, you can use these questions. Please bear in mind that they are just a start and it is recommended to go deeper into analysis:

- Did you define a Data protection officer?
- Is your staff trained regarding privacy protection?
- Do you have an internal data privacy policy?
- On your Web-Presence: Do you have a data privacy policy that can be read by users?
- Did visitors and employees agree to their personal data collection, e.g. during registration or regarding video surveillance? Are people made aware, e.g. by signs, that their video is being recorded?
- Are sufficient contractual regulations with vendors and suppliers in place regarding privacy protection? Should an audit be conducted? Is the business partner

obligated by contract to inform you during a data breach?
- Is data collection reduced to a required minimum? At the point of data collection, is the user informed about the data collection?
- Is access to personal data restricted to authorized personnel?
- Before sharing personal data, is the explicit consent of the user being collected?
- Are confidentiality clauses in place with personnel who have access to personable identifiable information?
- Is personal identifiable information, that is not required for their purpose anymore, being deleted in time or at least anonymized?
- Is a Self-Assessment of Security required by law for international data transmission and if yes, has it been conducted and documented?

Common pitfalls and tips

- While companies often try to consolidate their data in centralized data centers, due to the legal situation it is recommended to build up localized Chinese data storage at a minimum for Critical Information Infrastructures. Due to the ongoing implementation of the new rules introduced in 2017, generally a localized data storage is advisable.
- If you are outsourcing IT systems, you should clarify the ownership of data in your contracts.
- Due to the mixed Infrastructure of centralized IT and localized IT that many companies choose to use, be sure that especially or devices that are not managed in a centralized structure also follow encryption and backup regulations. Be also sure that encrypted data can be decrypted if the employee decides to leave the company and is not willing to share the password.
- At some point the user consent might be challenged: Make sure that you have appropriate documentation available.

Further Reading

Use the search engine of your choice to read more about:

- Cybersecurity Law
- Computer Information Systems Security Tiered Protection
- Telecommunication Networks Security Tiered Protection
- Network Security Check Practice Guide
- Data Transfer Measures.