Study on Classification of Data in Power Industry

Qin-yuan Li* and Jing Li
State Grid Zhejiang Electric Power Research Institute, China
*Corresponding author

Keywords: Electric power, Personal data, Enterprise data, Classification.

Abstract. The electric power industry is an important energy industry, and is related to economy and people's livelihood, so the data security issues is very important. Today is the era of cloud and big data, but the cloud environment and huge amounts of data cause the problem of data security, including the illegal acquisition and leakage of information and so on. In order to ensure data security, it’s necessary to classify the data and protect the key data according to the different needs. According to the domestic standard regulations and the internal norms of the state grid, the data which including user data and enterprise data is classified according to the subject. Data classification is divided into low-impact, medium-impact, and high-impact levels based on security objectives (confidentiality, integrity, availability). It is important for defining boundaries of data sharing and data open to classify data, protect the important and sensitive data in electric power industry and to improve the data security and access control of cloud platform.

Introduction

In recent years, with the maturity of cloud computing and big data technologies, [1] data integration and application based on big data technology have received more and more attention and development.[2] However, the collection of data has brought convenience and at the same time increased the difficulty and risk of data management.[3] As an important part of the key infrastructure, the data security protection of the power industry is a major issue that directly affects the people's livelihood. Data assets are increasingly becoming one of the most important assets in the power industry. Therefore, how to protect the data security in power industry has become an urgent problem to be solved.

This paper provides policy basis for the data security protection in the power industry from national law and internal standards; classifies the data from the two dimensions of user data and enterprise data, grades the data combined with national standards and internal norms. The results of data classification and grading will be an important reference to internal data protection of enterprise.

Analysis of National Standards

The laws and regulations mainly include personal information and enterprise information. The standards of personal information are as followed.

On November 5, 2012, the "Information Security Technology—Guidelines for Personal Information protection within Information Systems for public and commercial services (GBZ 28828-2012)” [4], which was spearheaded by the National Information Security Standardization Technical Committee, Officially released. The standard specifies requirements "handling of personal information should have specific, explicit and legitimate purposes, and should get permission of the subject of personal information and delete personal information after the purpose has been reached.” The most obvious difference of this standard is that for the first time, personal information is divided into general personal information and sensitive personal information according to the sensitivity level, and the management method of tacit consent and express consent is first proposed based on the result of the division of personal information. Tacit consent applies to the general personal information, as long as the main body of personal information does not express objection, the
information can be collected and used. The express consent is applied for sensitive personal information, the subject of personal information must know and give a clear authorization before the collection and use of sensitive personal information.

On December 28, 2012, the 30th meeting of the Standing Committee of the 11th National People's Congress passed the Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information. The significance of the "Decision" lies in the summing up the protection of personal information from some laws and regulations. The decision regulate the "personal information protection" from the level of legal norms for the first time.

In order to better protect personal information and important data, to protect the network information security, social security, national security, Combined with "National Security Law of the People's Republic of China" "Network Security Law of the People's Republic of China," and the relevant laws and regulations The Central Bureau of Internet Information and the relevant departments drafted the Measure for the Assessment of the Exit Security of Personal Information and Important Data (Exposure Draft)[6] (hereinafter referred to as the "Measure") for public comment on April 11, 2017. As a supplement to the “Assessment of the Exit Security of Personal Information and Important Data (Exposure Draft)”, “Information Security Technology—Guideline for data cross-border transfer security assessment(Exposure Draft)” led by the National Information Security Standardization Technical Committee was officially open to the community for comments. on May 27 2017. [7] The Assessment Guide sets out the assessment indicators and assessment methods of data cross-border transfer security, so that the government and enterprises themselves can conduct a comprehensive assessment of the data cross-border transfer security. This document standardizes the requirements, procedures, contents and results of data cross-border transfer security assessment and is applicable to the data cross-border transfer security assessment carried out by key information infrastructure operators. It also applies for relevant authorities of network safety and third-party assessment agencies to carry out data cross-border transfer security assessment, supervision and management work. The definition of "important data" in this guideline is as follows: The important data refer to the data collected by the Chinese government, enterprises and individuals in China and generated without any state secrets, but closely related to national security, economic development and public interests (including raw data And derivative data).There will be serious consequences once they have been disclosed, lost, abused, tampered with or destroyed, or aggregated, integrated and analyzed without authorization. In order to further guide the important data cross-border transfer security assessment, this paper gives the28 important data identification guidelines including oil and gas, coal, petrochemical, power, telecommunications, electronic information, steel, non-ferrous metals, equipment manufacturing, chemical industry, defense industry, other industries, geographic information, civil nuclear facilities, transportation, postal delivery, water conservancy, population health, finance , Credit, Food and Drugs, Statistics, Meteorology, Environmental Protection, Radio and Television, Marine Environment, E-Commerce and others

In addition, in the "Cyber Security Law" [8], which entered into force on June 1, 2017, "Chapter IV Network Information Security," "Article 40" "Article 41" "Article 42" also made a legal level of user information protection requirements, requiring "the user information collected should be kept strictly confidential, and establish and improve the user information protection system ", it clarifies the principle of responsibility, inform the principle of collecting principles, the use of principles, the principle of autonomy, the principle of integrity, safety management principles, notification, collection, use, independent choice, integrity and safety management.

In the protection of enterprise information, on April 27, 2010, the SASAC website promulgated the Interim Provisions on the Protection of Trade Secrets of State-owned-enterprises(SOEs)[9], requiring the central enterprises to incorporate the protection of trade secrets into risk management. The regulation clearly stipulates that SOEs must establish a corresponding information security support system to protect the trade secret information system of their own units. At the core, they continue to point to the security problems of sensitive data carrying trade secrets of various types of SOEs, Its core continues to be directed at the security of sensitive data carrying trade secrets of various types of
SOEs. Preventing information leakage has become the key and core of the protection and construction of trade secrets of SOEs.

In order to further enhance the technology prevention capability of trade secrets protection in SOEs and improve the protection level of trade secrets, the Confidentiality Commission of SASAC has taken the lead in formulating the "Guidelines for the Safety of Trade secrets Information Systems in SOEs [10] which was released on May 14 2012. This paper indicates that the protection of trade secrets of SOEs goes into the landing stage from the macro requirements. Its core continues to be directed at the security of sensitive data carrying trade secrets of various types of SOEs. Preventing information leakage has become the key and core of the protection and construction of trade secrets of SOEs.

Analysis of Enterprise Internal Norms

In order to better implement the Interim Provisions on the Protection of Trade Secrets of State-owned-enterprises and to protect the trade secrets of the State Grid Corporation of China and safeguard the legitimate rights and interests of the Company, the State Grid Corporation Confidentiality Commission, formulated the "State Grid Protection of Commercial Secrecy Regulations" according to the "State Secrets Law of the People's Republic of China" [11] and "Law of the People's Republic of China Against Unfair Competition" [12] and other laws and regulations, It clearly stipulates that according to the degree of importance and the degree of damage in economic interests once the information is leaked, the trade secrets identified as the core trade secrets and ordinary trade secrets,[13] The company operating information and technical information which belong to the scope of state secrets will be protected according to the law in accordance with the protection of state secrets.


Trade secrets refer to "operational information and technical information that is owned by the company and is not known to the public, can bring economic benefits to the company, is practical and is subject to confidentiality measures by the company." According to the degree of importance and the degree of damage in economic interests once the information is leaked, the trade secrets identified as the core trade secrets and ordinary trade secrets, Work secrets refer to "events and information generated by the company during its official activities and internal management and should not be disclosed to the public within a certain period of time, and once the company divulges, it will affect the normal operation and management order of the company and cause damage to the company."

Through the analysis of the relevant laws and regulations in China, we can find that the grading of power needs to focus on the user's personal data and take the sensitive data as the protection object. The key points include the following two points: Firstly, the national standards and regulations for data protection constraints are mainly reflected in two levels, one is the protection of personal information; one is the protection of trade secrets of SOEs. The former mainly include the Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information, the Network Security Law of the People's Republic of China, Information Security Technology—Guidelines for Personal Information protection within Information Systems for public and commercial services, the Information Security Technology Personal Information Safety norms ¦; the latter based on the "Interim Provisions on the Protection of trade Secrets of SOEs "and the" Guidelines for the Security of trade secrets Information Systems of SOEs ".

212
The internal provisions of the enterprise documents mainly cover the protection of internal trade secrets, which is an extension and supplement to the Provisional Regulations on the Protection of trade Secrets of SOEs. At the level of State Grid Corporation of China, the State Grid Corporation Confidentiality Commission has formulated the Provisions on the State Grid Protection of trade Secrets and the Regulations on the Intensified Scope of State Grid Corporation of China (Trial) [14].

**Data Classification and Grading**

We can classify the data information according to the data subject, which is mainly divided into two categories: user data and enterprise data. The following two aspects from the user data and enterprise data to introduce data classification and grading.

**Classification of User Data**

User data refers to "information recorded electronically or in other ways that identifies a natural person, including information about the behavior, location, biometrics, etc., either alone or in combination with other information." Please refer the details of definition and scope of personal/user data to the national standard GBZ 28828-2012 Information Security Technology Public and Business Services Information System Personal Information Protection Guide "and" GB/T xxxx-xxxx Information Security Technology Personal Information Security Specifications "(Exposure Draft).[15]

According to the Personal Information Protection Guidelines (GBZ 28828-2012), personal data can be further divided into sensitive personal data and general personal data. Sensitive personal data means "personal information that adversely affects the subject of the personal information once it is disclosed or modified." General personal data refers to the part of personal information except personal sensitive information.

Sensitive personal information refers to the information that is closely related to personal interests. Once leaked, public disclosed or abused , it may jeopardize personal and property safety, impair personal reputation, harm physical and mental health, and lead to discriminatory treatment. Under normal circumstances, ID number, bank card number, health status, biometric information, etc belong to sensitive personal information. It can be judged from the following perspectives whether it belongs to sensitive personal information:

Leakage: Once the disclosure of personal information happens, which cannot be controlled by the subject of personal information and the organization information using personal, the personal information will be out of control of its subject, and the proliferation and use will also be out of control in an unknown state. When some personal information is leaked, and then directly used or analyzed in association with other information against the wishes of the main body of personal information, it may pose a significant risk to the personal interests of personal information and should be judged as sensitive personal information. For example, a copy of the ID card of the personal information subject is used by others for the registration of the real name of the mobile phone number card and the bank account opening card.

Public disclosure: The personal information which once spread beyond the scope authorized by the subject of personal information and will pose a significant risk to the rights and interests of the subject of personal information should be judged as sensitive personal information. Such as sexual orientation, deposit information, history of infectious diseases.

Abuse: Certain personal information is used when it is beyond the reasonable limits of authorization (such as changing the purpose of processing and expanding the scope of processing) may pose a significant risk to the personal interests of personal information. For example, in the absence of personal information subject authorization, health information is used for insurance company marketing and determining individual premiums.
**Classification of Enterprise Data**

Enterprise data refers to "business information and technical information that is owned by the enterprise and is not known to the public and can bring economic benefits to the enterprise, which is practical and confidential by the enterprise."

According to the Interim Provisions on the Protection of Trade Secrets of SOEs, enterprise secrets include trade secrets and work secrets.

Enterprise data classification should have a global consciousness. According to the enterprise's current situation and the data classification of various departments such as production, business and commerce, classifies the data with the enterprise management information system.

**Data Grading**

Data grading is based on certain principles, the purpose of data grading is data management according to the grading results. Therefore, the data grading will be based on the following basic principles:

1. The principle of independent grading, all departments of data should be independent in accordance with the grading method to grade various types of data;
2. The principle of clear demand. After determining the levels for various types of data, departments should clarify the opening and sharing requirements at each level, the scope of data distribution at each level and whether the data needs to be decrypted or desensitized at each level.
3. The principle of clear boundaries, the data grading is divided according to the sensitivity of the data.
4. Higher level has priority. if the attributes or fields in the same batch of data have different levels of classification, safety control should be implemented in accordance with the highest rated attribute or field level.

We categorized the data into Low-Impact, Moderate-Impact and High-Impact levels based on security objectives (confidentiality, integrity, availability). Confidentiality refers to preventing information leakage and illegal access to protect personal and enterprise data. Integrity refers to preventing inappropriate modification and damage of information and ensuring the authenticity and non-repudiation of information. Availability refers to ensuring the reliability and timeliness of information.

This definition is based on the assumption that the security objectives of information systems will change due to the occurrence of certain events and grades the data according to different events on the impact of different safety goals.

Low-Impact Level: Unauthorized disclosure of data has a detrimental (Limited) impact on the organization's operations, the organization's assets, or individuals

Moderate-Impact Level: Unauthorized disclosure of data has a serious adverse effect on the organization's operations, the organization's assets, or individuals

High-Impact Level: Unauthorized leaks of data have a devastating or catastrophic adverse effect on the organization's operations, the organization's assets, or individuals

Therefore, according to the relevant standards and laws, based on the data security goals and potential negative impacts, we grade the data into 3 levels

High sensitivity level: The disclosure of data will make company's interests suffered particularly serious losses

Moderate sensitivity level: The disclosure of data will make company's interests suffered large losses.

Low sensitivity level: The disclosure of data will affect the normal operation and management order and make company's interests suffered passive losses.

**Inclusion**

This article analyzes the policy basis of data protection from national laws and regulations and enterprise internal norms. From an enterprise perspective, data protection solutions require a combination of efficiency and cost. The first step is to clarify the type of data to protect, classify and grade the data, protect and Implement hierarchical protection and control. This paper classifies the
data from user data and enterprise data, with user personal data as the key point and sensitive business secret data as the core, gives guideline and reference of data classification and grading. Each enterprise can Refine Improvements according to its internal data characteristics, thus the regulation of data classification and grading with enterprise’s own characteristics will be formed. It is important for defining boundaries of data sharing and data open to classify data, protect the important and sensitive data in electric power industry and to improve the data security and access control of electricity companies.

References