大成 DENTONS

Data Compliance in the Energy and Chemical Industries (III)

Grow | Protect | Operate | Finance

Sort date: 2022.02.22

In the previous two articles, from **data processor perspective**, we illustrated how energy and chemical enterprises assess whether or not they may be classified as critical information infrastructure operators ("**CIIOs**"), and from **data classification and grading perspective**, we also discussed how energy and chemical enterprises manage relevant industrial data through classification and grading approaches. This article will further explore how energy and chemical enterprises should fulfil their data compliance obligations from the perspective of various application scenarios of industrial data.

In the last article, we mentioned that the Ministry of Industry and Information Technology promulgated the *Administrative Measures for Data Security in the Sectors of Industry and Information Technology (for Trial Implementation) (Draft for Comments)* (the "**Draft Measures**") on 30 September 2021 to seek the comments from the public for the first time. And on 10 February 2022, a second version of the Draft Measures was released to solicit public comments again.

Although the Draft Measures is still soliciting public comments and has not yet come into effect officially, as a sectoral rule specifically regulating the data compliance in the industrial field, the Draft Measures expressly states that it applies to the data generated and collected in the course of R&D and design, production and manufacturing, business management, operation and maintenance, platform operation and other processes in all sectors and fields of industry, and sets forth different and specific requirements on different application scenarios that energy and chemical enterprises may fall into in the process of data compliance. Hence, this Draft Measures deserves attention from enterprises.

1. For different grades of data, how should energy and chemical enterprises fulfil compliance requirements under different application scenarios?

The Draft Measures, in consideration of industrial data at different grades and different application scenarios, stipulates detailed requirements on data protection, and provides specific practical guidance for relevant energy and chemical enterprises as data processors on their fulfilment of data compliance obligations. The following chart respectively sets different compliance requirements in the Draft Measures on general data, important data and key data[1] under main application scenarios, for your reference:

1. For the grading rules of industrial data, i.e. which data should be classified as general data, important data and key data, please refer to our second article of this series.

Data Grade Scenarios	All data (including General Data, Important Data and Key Data)	Important Data and Key Data
Data Collection	• Adhere to the principle of legality and properness, and shall not steal or collect data in an illegal way; • Adopt the corresponding security measures based on the grade of data security;	• Strengthen the management of the personnel and equipment collecting the important data and key data, and record the time, type, quantity, frequency and flow of collection; • For indirect collection of important data and key data, enterprises shall sign relevant agreements, letters of commitment or other documents with data providers to specify their respective legal liability.
Data Storage	Store data in accordance with the law or the method and duration agreed with the users.	• Secure storage by adopting measures such as verification technology and cryptography, and not directly provide public information network access to the storage system. Implement data disaster recovery backup and storage medium security management, and conduct data recovery testing regularly. • For key data, remote disaster recovery backup shall also be implemented.
Data transmission	Clarify the scope, category, conditions, and procedures of the provision and enter into data security agreements with the data recipients;	Assess or verify the data security protection capability of the data recipients, and take necessary safety protection measures.
Data Destruction	• Establish a data destruction system specifying the objects, rules, procedures, technology and other requirements of destruction, and record and file the destruction activities; • In case individuals or organizations request to destroy the data in accordance with the laws or the contracts, the enterprises shall destroy the relevant data per such request.	Timely file update with local competent department of industry and information technology, and not recover destroyed data for any reason or in any way.
Data cross-border transfer	Cross-border transfer security assessment is not mandatorily required for general data	In principle, important and key data shall be stored within China; if there is a need to transfer data to overseas, a security assessment shall be conducted in accordance with laws and regulations.
Data Transfer	Specify the transfer plan for any data transfer due to merger, restructuring, bankruptcy and other reasons, and notify the affected users by telephone, text message, email, announcement or other method.	Timely file update with local competent department of industry and information technology.
Entrustment	In case an enterprise entrusts others to carry out data processing activities, the data security responsibilities and obligations of the entrusting party and the entrusted party shall be specified under a written agreement.	Assess or verify the entrusted party's capability and qualification on data security protection.

2. Are there any other requirements should energy and chemical enterprises pay additional attention to?

In addition to the compliance requirements on different grades of data under different application scenarios, we recommend that energy and chemical enterprises (especially those processing important data and key data) should also pay attention to the following requirements under the Draft Measures in the course of overall processing of industrial data:

2.1 First responsibility of legal representative

For an energy and chemical enterprise which processes important data and key data, the Draft Measures stipulates for the first time that the legal representative or the person in charge of such enterprise shall be the first responsible person for data security, and the management member who is in charge of data security in such enterprise shall take direct responsibility for data security. This provision further clarifies the definition and scope of the "person directly in charge and other directly responsible persons" in the PRC Data Security Law.

In case an energy and chemical enterprise illegally processes data, and the "person directly in charge and other directly responsible persons" of such enterprise shall be imposed with the administrative penalty pursuant to the PRC Data Security Law or other relevant laws and regulations, the legal representative and the management member in charge of data security of such enterprise shall be the first subjects of such penalty. The establishment of such first responsibility of the legal representative will force energy and chemical enterprises to pay more attention to the compliance management of industrial data.

2.2 Filing and Approval Requirements

For an energy and chemical enterprise which processes important data and key data, the Draft Measures also proposes for the first time a filing system, i.e., such enterprise shall file the catalogues of the important data and key data with the local competent department of industry and information technology. The items to be filed include without limitation the data category, grade, scale, purpose and method of processing, scope of use, responsible party, external sharing, cross-border transmission, security protection measures, and other basic information. However, the content of data itself is not required to be filed.

Local competent department of industry and information technology shall, within 20 working days after the submission of filing application by enterprises, complete the examination and issue a filing receipt if such filing is in line with the relevant requirements, and meanwhile report the filing situation to the Ministry of Industry and Information Technology; if such filing is not approved, it shall inform the filing applicants and state the reasons in time.

If the category or scale of important data or key data changes more than 30%, or other filed records substantially change, the enterprise shall initiate update filing within three months after the occurrence of such change.

Such filing system is established based on the fact that industrial data, especially important data and key data hereof, is mostly related to the national economic operation and people's livelihood, which is one of the data types under national key administration. Enterprises report the information of important data and key data through this filing system, which will facilitate the national management and control in terms of data security and compliance.

3. What are the general suggestions on data compliance for energy and chemical enterprises?

Having said the above, by analysing the data compliance requirements under the Draft Measures, we can apparently see that the Chinese government adopts an attitude of "stronger administration" and "strict requirements" towards industrial data security and compliance. Along with the future promulgation of other implementation rules in data security protection field, if energy and chemical enterprises have not established their own data compliance system yet, they may face more compliance pressure and operational risks in the future operation. Therefore, before the Draft Measures officially takes effect, we suggest energy and chemical enterprises should, as soon as possible,

3.1 Identify own roles:

conduct internal assessment, and judge whether or not they are general data processors or CIIOs;

3.2 Conduct data classification and grading:

carry out classified management of data processed by enterprises, and grade data into three levels: "general data", "important data" and "key data".

3.3 Conduct differentiated management:

distinguish different application scenarios and data processing procedures, and manage different levels of data differently.

3.4 Set data compliance guidelines:

set compliance guidelines focusing on important data, key data, and commonly used application scenarios that may be involved in by sorting out the types of industrial data and the data processing procedures, and build the overall data compliance system.

3.5 Carry out data compliance rectification:

in addition to taking the above-mentioned measures, if any non-compliance in data management is found, data compliance rectification shall be carried out immediately, so as to make full preparation in advance to cope with the possible impacts after the Draft Measures officially takes effect.

To sum up

This is the finale of the series article titled "Data Compliance in the Fields of Energy and Chemical Industries". If you have any comments or questions, please do not hesitate to contact us. We would be happy to further explore and communicate with you. We will also continue paying attention to the legislation developments on data compliance in the energy and chemical industries and will provide you with professional insight timely.

About the authors

Nancy Sun
Senior Partner
D +86 21 3872 2122
nancy.sun@dentons.cn

Amanda Guo
Partner
D +86 21 3872 2106
amanda.guo@dentons.cn

Sunny Qin
Senior Associate
D +86 21 5878 5173
tian.qin@dentons.cn

CSBrand-86138-Data Compliance in the Fields of Energy and Chemical Industry_1-02 — 29/04/2022