

Notice on protecting personal information and using big data to support joint prevention and control

12:40, February 9, 2020 Source: [China Netcom](#)

[\[Print\]](#) [\[Error Correction\]](#)

Provincial, autonomous region, and municipality cybersecurity and informatization committees, and relevant ministries and commissions of central and state organs:

In order to protect the personal information in the joint prevention and control of the new type of coronavirus infection and pneumonia, actively use big data including personal information to support the joint prevention and control. With the consent of the Central Cyber Security and Informatization Commission, the relevant matters are notified as follows :

1. All localities and departments should attach great importance to the protection of personal information, except for those agencies authorized by the State Council 's Health and Health Department in accordance with the "Internet Security Law of the People 's Republic of China", "The Law of the People 's Republic of China on Prevention and Control of Infectious Diseases" and "Regulations on Public Health Emergencies" No other unit or individual may use personal information on the grounds of epidemic prevention and control or disease prevention without the consent of the person being collected. Where laws and administrative regulations provide otherwise, they shall be implemented in accordance with them.
2. The collection of personal information necessary for joint prevention and control should refer to the national standard "Personal Information Security Regulations" and adhere to the principle of minimum scope. The collection object is limited to key groups such as diagnosed persons, suspects, and close contacts in principle, and is generally not targeted at specific areas. To prevent de facto discrimination against specific geographic groups.
3. Personal information collected for epidemic prevention and control and disease prevention shall not be used for other purposes. No unit or individual may disclose personal information such as name, age, identity card number, phone number, home address, etc. without the consent of the person being collected, except for the joint defense and joint control work, except for desensitization.
4. The institution that collects or holds personal information shall be responsible for the security protection of personal information, and adopt strict management and technical protection measures to prevent theft and leakage.
5. Encourage capable enterprises to actively use big data under the guidance of relevant departments to analyze and predict the flow of key populations such as diagnosed persons, suspects and close contacts, and provide big data support for joint prevention and control.
6. Any organization or individual who discovers the collection, use, or disclosure of personal information in violation of laws and regulations may report it to the online information and public security departments in a timely manner. The network information department shall promptly

handle the illegal collection, use, and disclosure of personal information in accordance with the Cyber Security Law of the People's Republic of China and related regulations, as well as incidents that cause a large amount of leakage of personal information; public security organs involved in crimes shall be severely cracked down in accordance with the law.

Central network security and information

Committee office

February 4, 2020

http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm