No.	Statutory Circumstances	Definitions and Observations
1.	When a data processor exports any **important data**	The Measures broadly define "important data" as "data that may endanger national security, economic operation, social stability, public health and safety once it is tampered with, destroyed, leaked, or illegally obtained or used." The concept of important data was first raised in the Cybersecurity Law, under which network operators in China are required to categorize data and formulate backup and encryption measures for the protection of "important data." The Data Security Law further requires that business operators that process "important data" must appoint a responsible person and establish a specific internal department for important data protection, carry out risk assessments on a regular basis and report the risk assessment results to the competent authorities.
2.	When a **critical information infrastructure** (CII) operator exports any personal information	CII refers to important network facilities and information systems in important industries and fields, such as public communication and information service, energy, transportation, water resources, finance, public services, e-government affairs, science, technology and industry for national defense, as well as other important network facilities and information systems of which destruction, loss of function and data divulgence may seriously endanger national security, people's livelihoods and public interests. CII operators fall within a narrower set of data processors that operate critical information infrastructure as defined above.
3.	When a data processor that processes personal information of **one million individuals or more** exports any personal information	This scenario targets a data processor that processes personal information of one million individuals or more during its operation, such as large internet platforms and APP operators. Regardless of how many individuals' personal information will be exported, if the data processor processes personal information of at least one million individuals, any export of personal information by the data processor is subject to security assessment.
4	When a data processor who has, since January 1 of the previous year cumulatively exported **personal information** of more than 100,000 individuals, or the **sensitive personal information** of more than	This scenario targets a data processor based on the number of individuals whose personal information or sensitive personal information has been exported by the data processor within a certain period of time. "Sensitive personal information" refers to personal information, of which leakage or unlawful use may lead to discriminatory treatment or serious damage to personal or property safety, including race, ethnicity, religious beliefs, personal biometrics,

No.	Statutory Circumstances	Definitions and Observations
	10,000 individuals exports any personal information	medical health information, financial accounts, and personal whereabouts, etc., including personal information of minors younger than 14 years old. Hospitals, schools, banks and other organizations that typically process sensitive personal information are more likely to be the focus of this scenario. Also, multinational companies that have many local employees in China whose personal information and/or sensitive personal information have been shared by its offshore headquarters or affiliates during the years following January 2021 might also be included in this threshold.
5.	Other circumstances to be designated by the CAC that require security assessment	This leaves room for the CAC to introduce other circumstances where it believes a security assessment is necessary.