

Guidelines for Data Sharing between Financial Institutions

Contents of Guidelines	Description
<p>Article 1</p> <p>The Guidelines were established to increase convenience for customers of financial institutions, enhance risk management of financial institutions, and promote cross-sector cooperation between financial institutions.</p> <p>The sharing of data between financial institutions shall be conducted in accordance with the Personal Data Protection Act and the Guidelines, except in cases where data sharing is permitted by other regulations and such regulations shall apply.</p> <p>The other regulations that allow data sharing referred to in the preceding paragraph shall be compiled and disclosed on the website of the Financial Supervisory Commission.</p>	<p>I. The Financial Supervisory Commission (FSC) expressly states the purpose for the establishment of the Guidelines in Paragraph 1 is to increase convenience for customers of financial institutions, enhance risk management of financial institutions, promote cross-sector cooperation between financial institutions. The guideline is intended to enhance consumer rights and interests, facilitate the reasonable use of customer data based on the principles for ensuring information security, and promote data sharing mechanisms between financial institutions. The Guidelines were established to provide administrative guidance.</p> <p>II. The reasonable use of customer data by financial institutions shall be based on the Personal Data Protection Act. Financial institutions may also use such data for specific purposes and for other purposes in accordance with laws or the regulations or ordinances with specific authorization based on laws. Financial laws and regulations also governing the use of customer data, in addition to requires the consent of customers, financial laws and regulations also requires the reasonable use of customer data in accordance with laws(e.g., Money Laundering Control Act), internal control regulations for promoting public welfare or strengthening risk management and legal compliance. To promote reasonable and effective use of data, data sharing already permitted between financial institutions in accordance with</p>

	<p>the aforementioned regulations can be conducted accordingly. The FSC thus expressly states in Paragraph 2 that where data sharing is permitted by other regulations, such regulations shall apply. If the data sharing is not explicitly provided in existing regulations or if no restrictions are imposed, it may be conducted in accordance with the Personal Data Protection Act and the Guidelines.</p> <p>III. The FSC expressly states in Paragraph 3 that the other regulations allowing data sharing referred to in the preceding paragraph shall be compiled and disclosed on the website of the Financial Supervisory Commission for reference or convenient review by financial institutions. Any future adjustment in regulations shall also be updated on the website.</p>
<p>Article 2</p> <p>The terms as used in these Guidelines are defined as follows:</p> <p>I. Financial institutions: They refer to financial holding companies, banks, credit cooperatives, bills finance companies, trust enterprises, electronic payment institutions, post offices engaging in postal remittances or simple life insurance business, securities firms, securities investment trust enterprises, securities finance enterprises, securities investment consulting enterprises, futures commission merchants, leverage transaction merchants, futures trust enterprises, managed futures enterprise,</p>	<p>I. The FSC expressly states the scope of financial institutions and subsidiaries of financial institutions specified in the Guidelines.</p> <p>II. Financial institutions refer to the domestic financial institutions specified in Subparagraph 1 and branch companies in Taiwan of foreign financial institutions incorporated and registered in accordance with foreign laws.</p> <p>III. Where financial institutions are permitted to share data with their foreign subordinate companies or branches for the purposes of anti-money laundering in accordance with existing regulations, such regulations shall apply. However, data</p>

<p>futures advisory enterprises, and insurance companies. However, they do not include the foreign branches of these institutions.</p> <p>II. Subsidiaries of financial institutions: They refer to subordinate companies controlled by financial institutions in the preceding subparagraph in accordance with Article 369-2 of the Company Act that meet the definitions of financial institutions in the preceding subparagraph. However, they do not include subordinate companies or branches of financial institutions in foreign countries.</p>	<p>sharing conducted in accordance with these Guidelines may not be transmitted across borders. The FSC therefore specifies in Subparagraph 1 and Subparagraph 2 that the scope does not include subordinate companies or branches of financial institutions in foreign countries.</p>
<p>Article 3</p> <p>When financial institutions share data in accordance with the Guidelines, they shall establish internal control regulations based on the following principles:</p> <p>I. Data sharing must be based on a specific and appropriate purpose and must comply with laws and meet moral standards.</p> <p>II. If the data shared consist of identity verification data or negative data, which has a greater impact on the rights and interests of customers, financial institutions must conduct necessary verification or provide other measures to strengthen customer data protection.</p> <p>III. Participants and their employees must be authorized for the data sharing process and must have sufficient knowledge of related regulations, internal controls regulations, and the terms and conditions for data sharing.</p>	<p>I.Paragraph 1 expressly states that financial institutions must establish internal control regulations for data sharing conducted based on the Guidelines, and specified the principles for compliance, including the purpose of sharing, legality, eligibility of related employees, data management, review, authorization, method for processing issues with material impact on customer rights and interests, and dispute resolution procedures.</p> <p>II.Examples of the moral standards specified in Subparagraph 1, Paragraph 1 are provided below:</p> <p>(I)When using artificial intelligence to assess customer risks, financial institutions must seek to avoid potential biases.</p> <p>(II)Financial institutions shall not treat customers with the same conditions differently after analyzing customer data with artificial intelligence.</p> <p>III.The data with greater impact on the rights and interests of customers referred to in Subparagraph 2, Paragraph 1 include identity</p>

<p>IV. Financial institutions must establish appropriate management policies for data sharing, routine maintenance, data retention, access permissions, report management, and post-sharing processing.</p> <p>V. Financial institutions must establish clear risk-based internal audit and hierarchical accountability mechanisms based on their partners and the method of data sharing.</p> <p>VI. Financial institutions must ensure the security of the information system and data transmission.</p> <p>VII. Financial institutions must define internal standard procedures for receiving customer complaints and handling disputes in data sharing operations.</p> <p>The internal controls regulations in the preceding paragraph must be passed by the board of directors.</p>	<p>verification data, negative data, and other data that have not been made public.</p> <p>IV. Financial institutions may reference the "Rules Governing Exchanges of Negative Credit Data on Credit Extension Businesses by Financial Institutions through Joint Credit Information Center and Securities Firms through Taiwan Stock Exchange Corporation" for processing negative data. Financial institutions may also include relevant information that may affect customers' completion of financial transactions into the scope of negative data management in accordance with the nature of their business and the contents of the data sharing partnership.</p> <p>V. The overall internal control regulations for data sharing must be passed by the board of directors. Financial institutions may process individual partnerships based on the authorization of the board of directors and the hierarchical accountability mechanisms. The FSC therefore specified the requirement for hierarchical accountability mechanisms in Subparagraph 5, Paragraph 1, and the requirement for the overall internal control regulations for data sharing to be passed by the board of directors in Paragraph 2.</p> <p>VI. Data sharing application policy:</p> <p>(I) With regard to the data sharing application policy between financial institutions, the FSC focuses on the internal control system and its implementation. An application to the FSC for approval is not a necessary criterion. Prior to the implementation of the Guidelines,</p>
--	--

	<p>financial institutions have accumulated substantial experience and capacity in data sharing. Most current cases of data sharing between financial institutions, such as cross-selling or cooperative promotions, do not require applications for approval.</p> <p>(II)As the securities and futures companies had less regulatory basis and implementation in customer data sharing with other financial institutions in the past, if a securities firm or futures commission merchant conducts data sharing between Type III financial institutions, the first case requires approval by the FSC.</p> <p>(III)The FSC shall also gradually review or simplify procedures for those that currently require applications for approval and may change the necessary criterion for data sharing to the full implementation of an internal control system instead of obtaining approval.</p>
<p>Article 4</p> <p>A financial institution must disclose its privacy policy on the company website in order to share data between financial institutions. The content of the policy must include at least the name of the company sharing the data, purpose of sharing, customer data protection measures, and remedial measures for protecting customer rights and interests.</p>	<p>To increase the transparency of data sharing, accountability of partners, and customer trust, the FSC expressly states the minimum required contents of the privacy policy to be disclosed on the company website for data sharing between financial institutions. Financial institutions may disclose individual collaborative items and institutions in the form of attachments.</p>
<p>Article 5</p> <p>The eligible types for data sharing specified in the Guidelines include the three following types set forth below:</p> <p>I. Type I: Data sharing between financial holding companies and their</p>	<p>The FSC expressly states the eligible types for data sharing between financial institutions and classifies them into three types, including financial holding company groups, financial groups that are not financial holding companies, and</p>

<p>subsidiary financial institutions, and between subsidiary financial institutions of the financial holding company.</p> <p>II. Type II: Data sharing between a financial institution that is not a financial holding company and its subsidiary financial institutions, and between the subsidiary financial institutions of a financial institution that is not a financial holding company.</p> <p>III. Type III: Data sharing between financial institutions that are not included in the two types described above.</p>	<p>financial institutions that are not included in the two types described above.</p>
<p>Article 6</p> <p>Type I and Type II financial institutions may share data for the purpose of risk identification and risk management and must pay attention to the following matters:</p> <p>I. They must obtain the customers' consent in advance.</p> <p>II. The data that can be shared includes basic customer data, identity verification data, account data, transaction records of financial products or services, negative data, know your customer (KYC) data and inferred data from financial institutions, electronic communication history (e.g., IP address), or other data consented by customers and partner financial institutions for sharing.</p> <p>III. Financial institutions must ensure the protection of customer rights and interests, protection of personal data, and security of data transmission.</p> <p>IV. They must agree on at least the following items and rigorously carry out:</p>	<p>I. The FSC expressly states that Type I and Type II financial institutions may share data for the purposes of risk identification and risk management. The FSC also specified compliance matters including requirements for obtaining customer consent, scope of data sharing, protection of customer rights and interests, security of data transmission, and contents of the agreement.</p> <p>II. Subparagraph 1 expressly states that financial institutions must obtain the consent of the customer before sharing data, as the other subparagraphs of Paragraph 1, Article 20 of the Personal Data Protection Act do not apply to this Type. Before financial institutions obtain customer consent, they shall expressly inform customers of any of the purposes other than that originally specified, the scope of other use, and the impact of giving or not giving consent on their rights and interests (refer to Paragraph 2, Article 7 of the Personal Data Protection Act).</p> <p>III. The inferred data specified in Subparagraph 2 refer to data deduced</p>

<ul style="list-style-type: none"> i. The purpose of data sharing, the scope of data, and the frequency and manner of data collection, processing, and use. If customer consent is required, the method for informing the customer and obtaining consent must be specified. ii. A description of the participants of the data sharing and the division of labor and responsibilities of each participant. iii. Maintenance operations, data governance, risk management, and usage restrictions based on the nature of the data. iv. Related legal compliance matters for data sharing. <p>The financial holding company or the controlling financial institution may set up databases and manage the data sharing process in accordance with the regulations in Paragraph 2, Article 1 and the preceding paragraph. The financial holding company or the controlling financial institution may assign a subsidiary financial institution to process operations.</p>	<p>and derived by financial institutions from data provided by customers.</p> <p>IV. The KYC information shared between financial institutions based on this Article is provided for reference only and does not replace the KYC procedures that financial institutions are required to conduct in accordance with relevant regulations.</p> <p>V. To expand or grant financial institutions with greater flexibility in business operations and facilitate more effective implementation of risk management, the FSC expressly states in Paragraph 2 that the financial holding company or the controlling financial institution may set up databases and manage the data sharing processed in accordance with the regulations in Paragraph 2, Article 1 and the preceding paragraph, and may assign a subsidiary financial institution to process operations.</p>
<p>Article 7</p> <p>Type I, Type II, and Type III financial institutions may share data for the purpose of improving convenience for customers through means such as reducing the need for customers to enter data repeatedly, or for collaboration in business activities. They must also pay attention to the following matters:</p> <p>I. They must obtain the customers'</p>	<p>I. The FSC expressly states that Type I, Type II, and Type III financial institutions may share data for the purpose of improving convenience for customers (e.g., reducing the need for customers to enter data repeatedly), or for collaboration in business activities. The FSC also specified compliance matters including requirements for obtaining customer consent, scope of</p>

<p>consent in advance.</p> <p>II. The data that can be shared includes basic customer data, identity verification data, account data, transaction records of financial products or services, negative data, know your customer (KYC) data and value-added information from financial institutions, electronic communication history (e.g., IP address), or other data approved by customers and partner financial institutions for sharing.</p> <p>III. Financial institutions must ensure the protection of customer rights and interests, protection of personal data, and security of data transmission.</p> <p>IV. Financial institutions must establish business partnerships between them, agree on at least the following items , and rigorously carry out:</p> <ul style="list-style-type: none"> i. The purpose of data sharing, the scope of data, and the frequency and manner of data collection, processing, and use. If customer consent is required, the method for informing the customer and obtaining consent must be specified. ii. A description of the participants of the data sharing and the division of labor and responsibilities of each participant. iii. Maintenance operations, data governance, risk management, and usage restrictions based on the nature of the data. iv. Related legal compliance matters for data sharing. v. Starting and ending time of the 	<p>data sharing, protection of customer rights and interests, security of data transmission, business partners, and contents of the agreement.</p> <p>II. Subparagraph 1 expressly states that financial institutions must obtain the consent of the customer before sharing data, as the other subparagraphs of Paragraph 1, Article 20 of the Personal Data Protection Act do not apply to this Type. Before financial institutions obtain customer consent, they shall expressly inform customers of any of the purposes other than that originally specified, the scope of other use, and the impact of giving or not giving consent on their rights and interests (refer to Paragraph 2, Article 7 of the Personal Data Protection Act).</p> <p>III. The value-added information specified in Subparagraph 2 refer to data deduced and derived by financial institutions from data provided by customers.</p> <p>IV. The KYC information shared between financial institutions for the purpose of reducing the need for customers to enter data repeatedly or for collaboration in business activities is provided for reference only and does not replace the KYC procedures that financial institutions are required to conduct in accordance with relevant regulations.</p>
--	---

business partnership and the method for processing customer data upon the termination of the partnership.	
---	--