August 20, 2025

ChatGPT, Generative AI and Finance

So Saito

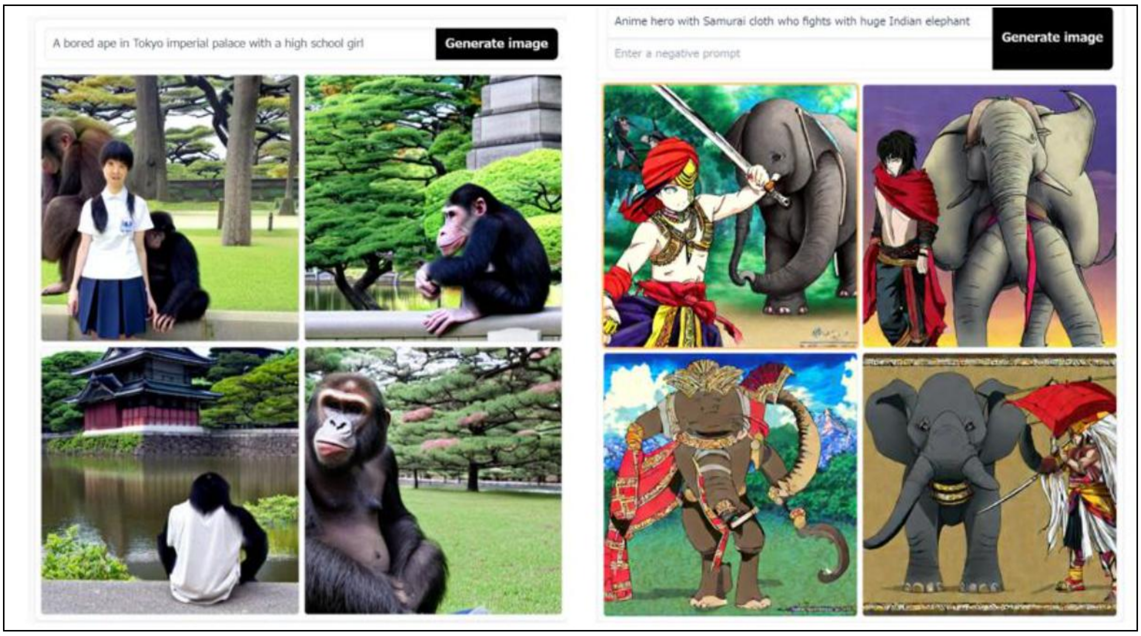
So & Sato Law Offices

1. What is Generative AI?

Generative AI refers to artificial intelligence that can automatically generate a variety of content, including images, text, audio, program code, and structured data.

Learning models that have learned large amounts of data through machine learning can easily generate images, music, text, and other content that resembles human creation.

From around 2022, image generation AI such as Midjourney and Stable Diffusion began to rapidly spread in the market, and from early 2023, generative AI specialized in natural language processing, such as ChatGPT and Bing, began to rapidly spread[1]



A bored ape in Tokyo imperial palace with a high school girl

Anime hero with Samurai cloth who fights with huge Indian elephant

Created on https://stablediffusionweb.com/ with the words "A bored ape in Tokyo imperial palace with a high school girl" and "Anime hero with Samurai cloth who fights with a huge Indian elephant

Examples of generative AI products include:

[1] In writing this article, we received valuable input from Tatsuto Fujii, Executive Officer of Microsoft Japan, who specializes in finance and technology.

Examples of generative AI products

Product name	Field	Product description
Midjourney, Stable diffusion, DALL・E etc	Image generation	AI that generates realistic/ artistic images based on text instructions
Artbreeder	Image generation	AI that generates new images from uploaded images or multiple images
Juke deck	Music generation	AI that generates original, copyright-free music by specifying genre, tempo, mood, etc.
Runway ML	Video generation	AI that can create videos by typing text
ChatGPT. Bing	Text generation	AI that responds in natural language to text input in natural language. Conversational agents, automated speech, machine translation, etc.
Catchy	Text generation	AI text creation tool specialized for Japanese

This article was also created using text generation AI such as ChatGPT. Specifically, we asked ChatGPT questions such as, "I'm thinking of writing a blog about financial institutions and generative AI. Please tell me the outline," and "Please give me some examples of generative AI products in table format," and then the output data was ① checked by a human, ② reconstructed by a human, ③ corrected by a human, and ④ added to by a human to finish it.

The data generated by text generation AI still contains many errors and cannot be used as is at present.

Currently, significant corrections and additions are made to the AI output data (i.e., it is not yet enough to eliminate human work), but even now it leads to a considerable improvement in work efficiency, and it is expected that it will become even faster and more accurate in the future.

2. Generative AI and Finance

With the rapid evolution of generative AI, many financial institutions are exploring the possibility of using AI to improve operational efficiency.

For example, financial institutions generally create a huge number of documents both for customers and internally. If generative AI can be used to streamline both customer and internal operations, such as creating explanatory documents and approval documents, it could lead to significant cost reductions. Furthermore, it could provide new services for customers, such as AI-based investment advisory services and automated portfolio optimization tools, and act as a sounding board for internal discussions.[2] It is also possible to use the answers from the chat AI as a reference to reconsider business decisions and organize your thoughts.

Applications of generative AI in the financial sector:

(1) Improving customer experience and marketing;

(2) Improving efficiency in customer-facing operations

(3) Improving efficiency in internal operations

(4) Investment advice and portfolio optimization

(5) Risk assessment and fraud detection

(6) Supporting discussions

On the other hand, the use of generative AI may give rise to new ethical and legal issues, such as the following:

AI and the Emergence of New Problems

(1) Bias Issues: In various types of screening, if the data used to train generative AI is biased toward a particular race or region, the AI may output biased results. This could lead to racial or regional discrimination.

(2) Privacy Issues: If financial services or products using generative AI require customer personal information, privacy concerns arise. Privacy must also be protected when using information generated by AI.

(3) Fraud Issues: Generative AI may be misused for sophisticated fraudulent activities. Examples include fraudulent transactions and phishing to steal personal information.

(4) Human Relationship Issues: As generative AI advances in automation, human labor and expertise may become less necessary. This could lead to job fluidity and unemployment. Furthermore, if AI decisions exceed human judgment, humans may become subordinate to AI, potentially shifting decision-making authority from humans to AI.

[2] For example, even with the current open generative AI, if you ask ChatGPT, "Please tell me what concerns you have about this company's rating," it will return a variety of answers, so although there are reliability issues, it can still be used as a sounding board.

As mentioned above, when it comes to generative AI and the financial sector, careful consideration is needed not only of technical issues, but also of ethical and legal issues and their relationship with humans.

3. Improving business efficiency through financial services and generative AI

Currently, the area in which financial institutions are most considering using AI is to improve operational efficiency.

From what we have heard, financial institutions have been contacting major AI companies in large numbers to ask about the use of AI and how to improve operational efficiency, and new developments are expected to take several months to complete.

For example, 1) AI can be used to streamline the creation of large volumes of documents, such as explanatory materials for customers, contracts, internal approval documents and various records, and applications and reports for regulatory authorities. 2) Chat AI can be used to automatically respond to customer inquiries (in text and audio), collect, record, and digitize the content of inquiries. 3) Large volumes of fictitious transaction data can be created to detect customer fraud.[3] ④ Possible actions include using AI to analyze information such as the borrower's past borrowing history and conducting loan screening.

One feature of AI use in financial institutions is that they do not use open databases like ChatGPT, but rather use dedicated databases that add their own company's own data to such open databases (using machine learning, etc.).

Using such dedicated databases has the advantage of providing answers that are more relevant to the business and ensuring confidentiality of business operations.

4. Machine learning by financial institutions, the Personal Information Protection Act, and confidentiality obligations

In order for generative AI to perform machine learning, it is necessary to feed the AI various types of data from your company (i.e. provide the AI with information, analyze it, and have it learn).

There are two possible options: either consuming the data in-house or providing the information to an external vendor to consume the data, but the data that financial institutions want to consume contains a lot of personal and confidential information, which

[3] It has been reported that "the UK Financial Conduct Authority (FCA) is using generative AI to develop AI that can detect fraudulent payments. They are using 5 million actual payment data sets as training data to generate large amounts of sample payment data." https://active.nikkeibp.co.jp/atcl/act/19/00146/072500086/

raises issues regarding the Personal Information Protection Act and confidentiality obligations.

Our current conclusions seem to be as follows, and we will consider each of them.

	In-house data use	Use of vendors for each part
When using personal customer information, the privacy policy states the purpose of use, such as "for research and development of new products and services through data analysis, etc."	It is within the scope of the purpose of use and possible	It is within the scope of the intended use, and confidentiality agreements must be concluded with possible third-party vendors.
When using personal customer information, the privacy policy simply states the purpose of use as "to improve services to customers"	This may be controversial, but it should be handled carefully. It is advisable to revise the privacy policy.	Same as left
No special confidentiality agreements have been signed regarding the use of corporate customer information	The relationship with the obligation of confidentiality that naturally accrues becomes an issue, but in principle, it is thought that there should be no problem.	There should be no problem if you sign a non-disclosure agreement with a third-party vendor.
We have signed special confidentiality agreements regarding the use of information from individual or corporate customers.	Depends on the content of the explicit confidentiality agreement, but contractually it is usually difficult	Same as left

Personal Information Protection Act

(1) When your company uses AI to use personal information

① Personal Information Protection Act and Purpose of Use

When processing data in-house, the question arises as to whether the processing is within the scope of the purpose of use. The Personal Information Protection Act requires that when handling personal information, the purpose of use must be specified as much as possible (Article 17, Paragraph 1 of the Personal Information Protection Act). [4] Unless the consent of the individual is obtained, personal information cannot be handled beyond the scope necessary to achieve the specified purpose of use (Article 18, Paragraph 1 of the same Act). Furthermore, when personal information is acquired, unless the purpose of use has been publicly announced in advance, the individual must be promptly notified of or publicly announced the purpose of use (Article 21, Paragraph 1 of the same Act).

If the use of AI falls outside the scope of the previously set purpose of use, the purpose of use must be changed. If the use of AI falls within a scope that can be reasonably deemed to be related to the previously set purpose of use, it is sufficient to notify the individual or make it public (Article 21, Paragraph 3 of the same Act). On the other hand, if the change goes beyond the permitted reasonable scope, the purpose of use must be set again after obtaining the individual's consent for use with AI.

In addition, if the consent of the individual is required when revising the privacy policy as described above, the provision on the procedure for changing standard terms and conditions under the Civil Code (Article 548-4 of the Civil Code), which allows standard terms and conditions to be changed without consent in certain cases, is not considered to apply.[5] Therefore, in the case of online transactions, it is likely that procedures will be implemented such as clearly indicating the changes to the privacy policy in a pop-up window or similar and obtaining customer consent by clicking on the button.

② Specific examples of descriptions of the purpose of use in a privacy policy

For example, consider a case where a privacy policy simply states "to improve service to customers" and various personal information is used to improve the efficiency of customer-related operations. Even in such a case, it may be argued that "to improve service to customers" falls within the scope of the purpose of use, but from the customer's perspective, it would be unthinkable that their personal information would be used not just to provide service to themselves, but to improve service to customers in general (to improve business

[4] When specifying the purpose of use, it is desirable not to simply specify the purpose in an abstract or general way, but to specify it specifically to the extent that the individual can generally and reasonably imagine what business the personal information will ultimately be used for and for what purpose it will be used by the personal information handling business operator. (Personal Information Protection Commission, "Guidelines for the Act on the Protection of Personal Information (General Provisions)," p. 31, https://www.ppc.go.jp/files/pdf/220908_guidelines01.pdf)

[5] The drafters of the Civil Code amendments have stated that customer consent to the purposes of use of personal information and provision to third parties as stipulated in privacy policies is merely consent based on the Personal Information Protection Act, and is not intended to result in the formation of a contract, and therefore the regulations regarding standard terms and conditions do not directly apply to it (Hideki Muramatsu and Hironori Matsuo, "Practical Q&A on Standard Terms and Conditions," Shojihomu, 2018).

efficiency), and if so, it would be argued that this is an insufficient specification of the purpose of use and that the purpose of use should be changed.

Next, consider the case where a privacy policy stipulates "for the research and development of financial products and services through market research and data analysis," and various personal information is used to improve the efficiency of customer-facing operations. In this case, although it is not explicitly stated that the analysis is performed using AI, it is reasonable to expect that some kind of data analysis will be performed using large amounts of customer personal information, and that the results will be used to research and develop financial products and services. Therefore, it is generally safe to assume that use with AI also falls within the scope of the privacy policy's intended use.

In any case, you will need to consider the specific wording of the privacy policy and the purpose of use, and consult with your legal department.

(2) When providing personal information to a third-party vendor and allowing them to use the personal information in AI

① Personal Information Protection Act and Third-Party Provision

When providing personal information to other companies, such as vendors, to feed it to AI, in addition to the above, the question of whether or not this falls within the scope of third-party provision arises.

In principle, when providing personal data to a third party, a personal information handling business operator must obtain the consent of the individual (Article 27, Paragraph 1 of the Personal Information Protection Act).

However, if a business operator outsources all or part of the handling of personal data to a third party within the scope necessary to achieve the purpose of use, such outsourcing party will not be considered a "third party," and the individual's consent will not be required (Article 27, Paragraph 5, Item 1 of the Act). Therefore, if a business operator outsources the task of feeding personal information to an AI in order to build an AI service it provides, and the individual's consent is therefore not required. However, the outsourcer must provide necessary and appropriate supervision of the outsourcing party to ensure the safe management of personal data (Article 25 of the Act).

Furthermore, even when providing personal data to a specific person for joint use, the consent of the individual is not required if the individual is notified in advance of the joint use and certain information stipulated by the Personal Information Protection Act, such as the items of personal data, or if the individual is made readily available (Article 27, Paragraph 5, Item 3 of the Act). For example, joint use may occur when AI that uses personal data is used between group companies.

② Specific examples of providing personal data to vendors as part of outsourcing:
As a specific example of outsourcing that does not constitute third-party provision, for example, if the purpose of use in a privacy policy is clearly stated as "for the research and development of financial products and services through market research and data analysis, etc.", providing personal data to a third-party external vendor for analysis using AI could also be interpreted as "in connection with a business outsourcing all or part of the handling of personal data to the extent necessary to achieve the purpose of use."

③ Conclusion of a confidentiality agreement
Even if the Act on the Protection of Personal Information allows for the provision of personal data to a third party, it states that "the trustor must exercise necessary and appropriate supervision over the trustee to ensure the safe management of personal data (Article 25 of the Act)," so naturally a contract imposing a confidentiality obligation on the third-party vendor will be necessary.

(3) Anonymously processed information and pseudonymized information

Even if the purpose of using the acquired personal information does not include analysis using AI, by processing the personal information to be fed to AI into anonymous processed information, it can be used for purposes other than those intended or provided to third parties without the consent of the individual.

Here, anonymously processed information means "information about an individual obtained by processing personal information in a certain way so that a specific individual cannot be identified, and the personal information cannot be restored" (Article 2, Paragraph 6 of the Act). However, when personal information is processed into anonymously processed information, processing must be carried out in accordance with standards set forth in the rules of the Personal Information Protection Commission (Article 43, Paragraph 1 of the Act, Article 34 of the Enforcement Regulations of the Personal Information Protection Act), such as deleting all or part of descriptions contained in the personal information that can identify a specific individual, deleting all personal identification codes, deleting codes that link personal information with processed personal information, and deleting peculiar descriptions, and it is thought that processing is often difficult.

Therefore, it may be possible to use pseudonymized information, which does not require more advanced processing technology than anonymously processed information.

Pseudonymized information refers to "information about an individual obtained by processing personal information in a manner that makes it impossible to identify a specific individual without comparing it with other information" (Article 2, Paragraph 5 of the Act on the Protection of Personal Information). Because pseudonymized information is less abstract than anonymously processed information, it has the advantage of maintaining the usefulness of personal information. Furthermore, unlike unprocessed personal information, it is possible to change the purpose of use beyond a scope that is reasonably recognized as being related to the previous purpose of use (Article 41, Paragraph 9 of the Act). However, unlike anonymously processed information, provision of pseudonymized information to third parties is prohibited in principle (Article 41, Paragraph 6 of the Act).

	Raw personal information	Pseudonymized information	Anonymously processed information
Processing	No processing	Processed so that a specific individual cannot be identified unless compared with other information	Processing to make it impossible to identify a specific individual and to restore personal information
Use for other purposes	It can be used within the scope of the specified purpose of use. In addition, it is not possible to change the purpose of use beyond the scope that is reasonably recognized as being related to the purpose of use before the change.	It can be used within the scope of the specified purpose of use. However, it is possible to change the purpose of use beyond the scope that is reasonably recognized as being related to the purpose of use before the change.	Unintended use is possible
Provided by a third party	In principle, consent from the individual is required	This is not permitted except as provided for by law (even if the individual's consent was obtained before the pseudonymized	In principle, the individual's consent is not required

		information was created). In addition, the provision that does not apply to outsourced work (Article 28, Paragraph 5 of the Act) applies.	

Duty of confidentiality

Financial institutions naturally have confidentiality obligations with their clients and other parties who provide them with information, and may also enter into confidentiality agreements that stipulate special confidentiality obligations when conducting special transactions such as M&A advice or securities underwriting. When using AI to analyze information, it is necessary to consider not only the relationship with the Personal Information Protection Act but also the relationship with such confidentiality obligations.

(1) Personal information without a special confidentiality agreement

With regard to personal information obtained without entering into a contract containing special confidentiality clauses, there is generally no argument that it naturally requires a confidentiality obligation greater than that stipulated in the Personal Information Protection Act. Therefore, I believe that there should be no problem with either in-house use or provision to a third party as long as it is carried out within the scope of the Personal Information Protection Act as discussed previously.

(2) Information about corporations that do not have a special confidentiality agreement

Regarding information on corporations acquired without entering into a contract containing a special confidentiality clause (for example, a corporation conducting transactions based on a normal banking transaction agreement), there is generally no argument that the confidentiality obligation towards a corporation is heavier than the confidentiality obligation towards an individual, so there will likely be no problem if the information is used within the company or provided to a third party within the same scope as for an individual.

(3) Information about individuals or corporations that have signed special confidentiality agreements

When financial institutions enter into special confidentiality agreements for M&A, IPO advice, securities underwriting, or other special contracts, many of these agreements contain clauses such as (1) not to use the information for purposes other than the IPO, and (2) not to disclose the information to third parties unrelated to the IPO. If such confidentiality agreements exist, it may be difficult to feed data to AI or provide the data to third-party vendors for purposes such as using generative AI to simplify the creation of materials for future IPO projects.

Regarding legal tech, for example, there is a debate as to whether uploading a contract file to a legal tech service for risk analysis constitutes disclosure of the contract to a third party, and if the contract stipulates a confidentiality obligation, does this constitute a breach of contract? Although there are arguments that this is in fact an implicit consent of the contracting party, and that since there is no actual damage, it is a matter of business judgment, etc.[6] the situation discussed in this section is far more related to actual cases than legal tech cases, and implied consent requires more careful consideration. Furthermore, the argument that there is no actual harm is likely to be made more carefully in the case of financial institutions, which are forced to be more cautious about compliance risks than general business companies.

At present, there may not be much need to feed AI large amounts of documents from parties that have confidentiality agreements, but considering that such needs may arise in the future, it may be necessary to consider the content of the confidentiality agreement templates that your company prepares.

5. Investment advice using generative AI

Legally, in order to engage in investment advisory and agency business, registration as a financial instruments business operator is required (Article 28, Paragraphs 3 and 29 of the Financial Instruments and Exchange Act).

According to Article 2, Paragraph 8, Item 11 of the Financial Instruments and Exchange Act, investment advice regarding financial instruments requires the following: 1) an agreement to provide advice verbally, in writing (with certain exceptions), or by other means regarding investment decisions based on an analysis of the value of financial instruments (meaning decisions regarding the type, brand, number, and price of securities to be invested in, as well as the choice, method, and timing of buying and selling, or

[6] CloudSign Blog: "Use of Contract Risk Analysis Service and Confidentiality Obligations" https://www.cloudsign.jp/media/20190716-legaltech-himitsuhojigimu/

decisions regarding the content and timing of derivative transactions to be conducted), and 3) the other party agreeing to pay a fee.

For example, if a generative AI is fed with information such as the past price movements, returns, and investment data of financial products, and as a result, it creates a text recommending an investment stock, etc., then such a text creation service may be considered an investment advisory business.

AI services that specialize in investment advice and are provided for a fee likely require investment advisory license certification. Currently, the "sale of computer software, such as investment analysis services," is understood to not constitute investment advisory services if the tools are available to anyone without additional support, such as through retail sales by retailers or download sales via networks. However, if the tool requires ongoing investment information or other support from a distributor, registration may be required (see the "Comprehensive Supervision Guidelines for Financial Instruments Business Operators, etc." below). Paid AI services specialized in investment advice are likely to secure their value through ongoing data provision and tuning by the AI provider, which may result in investment advisory services.

On the other hand, when financial institutions provide investment information free of charge for the purpose of general information provision, the requirement that "the other party pays compensation" does not apply, and therefore investment advisory services are not required.

The problem is that, although it is believed that AI has not yet evolved to that extent, if there is, for example, a general-purpose generative AI that also collects a large amount of information on financial products and, as a result, is able to provide investment advice, which is normally free of charge, but if you become a paid member you can get a quicker response, etc., would this be considered an investment advisory business?

In our opinion, even if one becomes a paid member of such an AI, this is not a fee for investment advice, but rather a way to obtain benefits such as speeding up AI in general, and therefore does not constitute investment advisory business. However, if AI continues to evolve in the future, further consideration will be needed as to whether this interpretation is appropriate.

Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. VII-3-1(2)②c

② Activities that do not constitute investment advisory and agency business

A. Activities that provide investment decisions based on the analysis of the values of securities or financial instruments (hereinafter referred to as "investment information, etc.") to an unspecified number of persons by methods that allow an unspecified number

of persons to purchase them
at any time. For example, persons who provide investment information, etc. by methods set forth in a to c below are not required to register as an investment advisory and agency business.
However, even if the target audience is an unspecified number of persons, it should be noted that registration is required in cases where highly individual and relative investment information. is provided by using information and communications technology such as the Internet, or where investment information cannot be purchased or used without membership registration (one-off purchases or use are not accepted).

a. Sales of newspapers, magazines, books, etc.
(Note) When these are displayed in the stores of general bookstores, kiosks, etc., and are available for anyone to freely view, decide, and purchase at any time. On the other hand, please note that registration may be required when selling reports, etc. that can only be purchased by applying directly to a dealer, etc.

b. Sales of computer software such as investment analysis tools
(Note) When the software is available for purchase by anyone at any time, freely, based on the investment analysis algorithms and other functions of the computer software, through over-the-counter sales by retailers or download sales via networks, etc. On the other hand, please note that registration may be required when it is necessary to receive data related to investment information, etc. or other support from a dealer, etc. on an ongoing basis when using the software.
（https://www.fsa.go.jp/common/law/guide/kinyushohin/07.html#07-03　）

Reservations

The contents of this article have not been confirmed by the relevant authorities and merely describe arguments that are reasonably considered legal. Furthermore, they represent only our current views, and our views may change.
This article is merely a compilation for this blog. If you require legal advice for a specific case, please consult with a lawyer.