Personal information handling policy

Article 1 (Personal Information Collected)

SM Entertainment Co., Ltd. (hereafter referred to as the "Company") collects the following personal information for membership registration, consultation, and service application.

① Collected information: Any usage history of Company-provided service such as, Name, login ID, password, email address, service use record, access log, cookie, access IP information, device identification number (device ID), PUSH token, fan club membership information and fan club grade, stamp issuance information, passport issuance information, etc.

※The above information about the device is in a format that cannot identify individuals, and the Company does not engage in activities that identify individuals based on the information collected.

② Methods of collection: website (membership registration, audition application, event participation, delivery request), written form, etc.

Article 2 (Purpose of Collecting and Using Personal Information)

Company uses the personal information collected for the following purposes.

① Implementation of terms and conditions relating to services provided and settlement of charges for services provided: Provision of contents, invoice delivery, purchase and payment of charges, and shipping of goods

② Membership Management: Personal identification due to the use of membership service, individual identification, prevention of illegal use or unauthorized use by a suspended member, confirmation of the intent to sign up, confirmation of age, confirmation of the consent of the legal representative of a person under 14 years of age whose personal information is being collected and personal identification of the legal representative in the future, handling of complaints, delivery of announcement, integrated ID management, membership service provision, card issuance, point saving and use settlement, VIP service provision

③ Use for Marketing and Advertisement: Development and specialization of new service (product), delivery of advertisement information such as events, provision of service and posting of advertisement pursuant to demographical characteristics, identification of access frequency, and statistics on Members' use of services

Article 3 (Retention and Usage Period of Personal Information)

In general, the Company destroys personal information without delay when the retention period has expired or when the information is no longer necessary, such as when the original purpose for collecting and using the information has been fulfilled. Nonetheless, if it is necessary to preserve information in accordance with the provisions of the applicable laws, the Company must retain the

member information for a specific period of time as specified by the applicable laws and regulations.

① Items to maintain: name, login ID, password, email address, service use record, access log, cookie, access IP information, payment record, preferred artist, i-PIN number, legal representative name, i-PIN CI, and member number

② Basis of retention: Act on the Consumer Protection in Electronic Commerce

③ Retention period: 3 years

A) Display / Advertising Records: 6 months (Act on the Consumer Protection in Electronic Commerce)

B) Record of contract or withdrawal of contract: 5 years (Act on the Consumer Protection in Electronic Commerce)

C) Record of payment and supply of goods: 5 years (Act on the Consumer Protection in Electronic Commerce)

D) Records of consumer complaints or dispute resolution: 3 years (Act on the Consumer Protection in Electronic Commerce)

E) Records of collecting, processing, and using credit information: 3 years (Credit Information Use and Protection Act)

Article 4 (Procedures and Methods for Destruction of Personal Information)

The following is the procedure and method for destroying personal information.

① procedure for destruction

A) After the purpose is achieved, the information entered by the Member for membership registration, etc. is transferred to a separate database (DB) or a separate filing cabinet in the case of paper, and stored for a period of time before being destroyed in accordance with Company guidelines and relevant laws and regulations.

B) Unless otherwise required by law, personal information transferred to a separate database will not be used for any other purpose than to be kept.

② Methods of Destruction

A) Electronically stored personal information is deleted using a technical method that prevents the record from being reproduced.

B) Personal information printed on paper is shredded or incinerated.

Article 5 (Entrustment of Collected Personal Information)

① For the smooth operation of the business, such as providing better services and facilitating customer convenience, the Company entrusts the following personal information handling tasks to an external professional company. During the contract period, the entrusted company keeps the Member's personal information. However, when the relevant laws specify a statutory retention period, the company keeps the Member's personal information for that time period.

② The Company ensures, through the entrustment contract, that the entrusted company

complies with personal information protection laws, keeps personal information confidential, does not provide information to third parties, accepts responsibility for accidents, and returns or destroys personal information after the entrustment period or after handling the information.

③ The service provider who has been entrusted with personal information
※ Depending on the change in service and the contract period, the entrusted company may change. When there is a change in the service, the company will notify Members in advance.

The company entrusted with personal information for the provision of the service	Amazon Web Service
Entrusted work and the purpose of entrustment	System management through AWS
Contact information of the entrusted company	Aws-korea-blog@amazon.com
The country to which personal information is transferred	Japan (AWS Tokyo Region)
Items of personal information to be transferred	All personal information collected in the process of providing services
Date of personal information transfer	Date of membership registration
Method of personal information transfer	Storage of personal information in AWS cloud computing environment
The length of time to keep and use personal information	Personal information will be retained until membership is withdrawn or until its expiration* date.

*Personal information expires when a Member has not used the service for one year, and measures such as storing information separately are implemented upon expiration.

Article 6 (Provision of Personal Information to Third Parties)

① The Company processes users' personal information only within the scope specified in the purpose of processing personal information, and only transmits personal information to a third party for cases under Articles 17 and 18 of the Personal Information Protection Act, such as the consent of the user and special provisions of the law. Otherwise, the Company does not provide personal information of users to a third party.

② order to provide smooth service in the following cases, the Company discloses personal information to third parties only to the extent necessary with the user's consent.

A)
Recipient of the information : SM Culture & Contents
Purpose of providing the information : Membership verification for member-exclusive reservation of concert and tour packages
Items of information provided : name, login ID, fan club membership information and fan club grade, stamp issuance data, and passport issuance data
Duration of storage and utilization : Until membership cancellation
A)
Recipient of the information : Yes24 Co., Ltd.
Purpose of providing the information : Membership verification pertaining to offline performance reservations
Items of information provided : name, name, login ID, fan club membership information and fan club grade
Duration of storage and utilization : Until membership cancellation
A)
Recipient of the information : SM BRAND MARKETING
Purpose of providing the information : Membership verification associated with the sale of exclusive items to members
Items of information provided : name, login ID, fan club membership information and fan club grade, stamp issuance data, and passport issuance data
Duration of storage and utilization : Until membership cancellation

③ In emergency situations such as natural disasters, infectious diseases, events/accidents that pose an imminent threat to life or body, and imminent property loss, the Company must provide personal information to relevant organizations without the consent of the subject of information, in accordance with the personal information handling and protection rules for emergencies jointly announced by the relevant government departments. Please click here* for additional details.

Article 7 (Rights of Users and Legal Representatives and Method of Exercising the rights)

① Users and legal representatives may inquire about or modify the registered personal information of themselves or children under 14 at any time, as well as request membership cancellation.

② Users or legal representatives can view and correct personal information or cancel membership after clicking 'Change Personal Information' (or 'Edit Member Information', etc.) to view and correct personal information of the user or children under 14 years of age or clicking 'Withdraw membership' to cancel membership (withdraw consent) and going through the identity verification process. Or, they can contact the person in charge of managing personal information via email, phone, or letter to make a request, which will

be handled expeditiously.

③ In the event of a request to correct errors in personal information, the information may not be used or disclosed until the correction has been made.

④ If incorrect personal information has already been provided to a third party, the result of the correction will be immediately communicated to the third party so that the correction can be implemented.

⑤ The Company ensures that personal information that has been canceled or deleted at the request of a user or legal representative cannot be viewed or used for any other purpose, in accordance with Article 3.

⑥ In the event of a request to suspend the viewing and processing of personal information, users' rights may be restricted in accordance with paragraphs 4 of article 35 and paragraph 2 of article 37 of the Personal Information Protection Act.

Article 8 (Matters Concerning the Installation, Operation, and Rejection of Automatic Collection of Personal Information)

The Company employs "cookies" that frequently store and retrieve user data. The server used to operate the Company's website stores the cookie as a text file on the user's computer's hard drive. The Company employs cookies for the purposes outlined below.

① Objective of using cookies

A) Targeted marketing and personalized services are provided by analyzing the access frequency and visit time of Members and non-Members, identifying users' tastes and interests and tracking their traces, and determining the level of participation in various events and the number of visits, etc.

B) Users have the option of installing cookies. The user can therefore configure their web browser to accept all cookies, check each time a cookie is saved, or reject all cookies.

② Methods to disable cookie settings

A) A user can accept all cookies by selecting the web browser's option, check each allowed cookie before saving it, or reject all cookies.

B) example of cookie configuration for Internet Explorer: select personal information on the Internet options by accessing tools at the top of the web browser

C) If a user declines to accept cookies, it may be difficult to provide services.

Article 9 (Measures for Personal Information)

① The Company develops and implements an internal management plan for the secure handling of personal data, as well as providing training.

② When it comes to users' personal information, the company takes technical precautions to ensure that it is not lost, stolen, leaked, altered, or damaged.

③ Personal information is managed on an internal network that cannot be accessed or infiltrated from the outside. Important information is safeguarded using a separate security

function that encrypts files and transmits data or employs a file lock function.

④ The Company is making every effort to secure the in-house network by using a firewall and an intrusion detection system for each server, as well as strengthening security by installing an access control system, in preparation for external intrusions such as hacking.

⑤ The Company protects personal information by installing a vaccine program that allows the personal information processing system and the personal information handler to continuously check for malicious programs such as computer viruses and spyware that have infiltrated the information devices used for personal information processing and to take the necessary precautions.

⑥ The Company limits the number of people who have access to a user's personal information to a bare minimum. The Company prepares internal procedures for access and management of personal information, implements access control and device lock, and ensures that employees are aware of and follow the procedures to ensure the safety of personal information.

⑦ The handover of tasks to personal information handlers is done in a secure manner. Even when employees join or leave the Company, their responsibilities for personal information mishaps are clarified.

⑧ Users are responsible for maintaining accurate information by verifying and managing the personal information they provide to the company. If a user uses another person's personal information without permission or infringes on another person's rights while using the Internet site, the user may face civil and criminal penalties as well as company sanctions.

⑨ The Company is not liable for any issues arising from the loss of personal information such as an ID, password, or resident registration number as a result of the user's negligence or Internet problems. As a result, each user must carefully manage his or her ID and password in order to protect his or her personal information and assume responsibility for its management. However, if the user's personal information is lost, leaked, altered, or damaged as a result of a company internal manager's mistake or a technical management accident, the Company will immediately notify the user and take appropriate measures and compensation.

Article 10 (Additional Use and Provision of Information)

① In accordance with paragraph 3 of Article 15 and paragraph 4 of article 17 of the Personal Information Protection Act, the Company may use and disclose personal information without the user's consent for the purposes of Article 14-2 of the Enforcement Decree of the Personal Information Protection Act.

② The Company considers the following factors when deciding on the additional use and disclosure of personal data without the user's consent.

1. Whether the additional use and disclosure of personal information is related to the initial purpose of collection

2. Whether additional use or disclosure of personal information is predictable in light of the circumstances under which the information was collected or established practices for handling the information.
3. Whether the additional use or disclosure of personal information violates the interests of users in an unreasonable manner
4. Whether necessary safety measures, such as pseudonymization or encryption, have been implemented

Article 11 (Obligation to Notify when Changing Privacy Policy)

① In the event that additions, deletions, or modifications are made to the content of this privacy policy in accordance with government policy or company policy, the company will provide 7 days' notice via the website prior to the revision.

② This policy goes into effect on June 20, 2022.
-Announcement date: June 13, 2022
-Effective date: June 20, 2022

③ The previous privacy policies are available for review below.
-Effective between April 22, 2019 and May 31, 2021
-Effective between May 31, 2021 and June 19, 2022

Article 12 (Complaint handling service related to personal information)

① The Company has designated the following department and a chief privacy officer in order to protect the personal information of customers and respond to complaints involving such information.
-A department responsible for customer service for the protection of personal information: FC Management Unit
-Telephone: 02-6240-9800
-email: privacy@smtown.com
-Name of Chief Privacy Officer: Choi, Byung-beom
-Telephone: 02-6240-9800
-email: privacy@stown.com

② Users can report any complaints regarding the protection of personal information that occur while using the Company's services to the chief privacy officer or the responsible department. The Company will respond promptly and adequately to user reports.
Users are encouraged to contact the following organizations to report or seek advice on other personal information violations.

1. Personal Information Dispute Mediation Committee (http://www.kopico.go.kr/ Tel: 1833-6972 without area code)
2. Personal Information Infringement Report Center (http://privacy.kisa.or.kr, 118 without area code)

3. Information Protection Mark Certification Committee (www.eprivacy.or.kr, 02-550-9531 to 2)
4. Korean National Police Agency Cyber Bureau (www.ctrc.go.kr, 02-3150-2659)

③ A person whose rights or interests have been violated by the disposition or omission of the head of a public institution with regard to requests made under Article 35 (viewing of personal information), Article 36 (correction / deletion of personal information), and Article 37 (suspension of processing of personal information, etc.) of the Personal Information Protection Act may request an administrative appeal pursuant to the provisions of the Administrative Appeals Act.

‣Central Administrative Appeals Commission: (without area code) 110 (www.simpan.go.kr)