1. Significance of the privacy policy

SM Entertainment Co., Ltd. (hereinafter referred to as the “Company”) legally processes and safely manages personal information of data subjects in compliance with the Personal Information Protection Act and related statutes or regulations.

Accordingly, in accordance with Article 30 of the Personal Information Protection Act, the following privacy policy is established and disclosed to inform data subjects of the procedures and standards for processing personal information and to promptly and smoothly handle complaints related thereto.

This privacy policy applies to the services provided by the company (hereinafter referred to as “services”) and the data subjects using the services (hereinafter referred to as “data subjects”).

2. Purpose of processing personal information

The company processes personal information for the following purposes: The personal information, which is processed by the company, will not be used for purposes other than the following, and if the purpose of use changes, necessary measures will be taken, e.g., obtaining separate consent from the data subjects in accordance with Article 18 of the Personal Information Protection Act.

[Recruitment]
- Candidate registration, verification of the identity of applicants, supporting materials for assessment of suitability for employment, document screening/interview, etc., and utilizing the DB (reference materials for continuous recruitment) of talented people
- Communication with applicants (delivery of notices and guidance, handling of inquiries related to recruitment)
- Benefit calculation
- Personnel management (nationality data - checking eligible visas for foreigners, management of veteran/disability status - giving preferential treatment when hiring)

[Reporting of unethical behavior]
- Receiving reports of unethical behavior and returning processing results

[Submit Business Inquiry]
- Receive and review business inquiries and provide feedback on the results.

[SMTOWN website and app, KWANGYA 119]
- Personal identification, confirmation of intent to join, identity verification, and age verification upon membership signup
- Handling complaints and grievances, delivering notices, and integrated ID management
- Provision of contents according to service contracts, delivery of event items, development and specialization of new services (products), provision of services and advertisements according to demographic characteristics, statistics on access frequency and members’ use of services, use of marketing and advertisements, and delivery of advertising information

[Audition (integrated)]

- Support for audition applications and audition-related procedures: Verification of the identity of audition applicants, checking the consent of the legal representative when processing the personal information of applicants under the age of 14, receipt of audition applications, checking duplicate applications, notification and disclosure of evaluation results, and use in training-related work
- Provision of other services: notification of the holding of an audition
- Responding to inquiries, receiving requests for counseling and returning processing results

3. Particulars of personal information to be processed

The Company collects the minimum amount of personal information as follows to provide smooth service, and does not collect 'sensitive information' without the consent of the data subject.

*Sensitive information: information that may infringe on the privacy of the data subject (personal information that may significantly infringe on the privacy of the user, such as thoughts, beliefs, political views, and health)

[Recruitment]

Required: name, email, cell phone number, gender, date of birth, nationality, address, academic background, profile photo, veteran status, self-introduction, application path, and curriculum vitae

Optional: work experience, overseas experience, language test scores, certificates, military service, and disability

Other: Portfolio and Pre-assignments (required or optional depending on jobs and job posting)

*Information, such as visit history during service use, job application records, records of fraudulent use, and terminal information (OS, screen size, and unique identifier of a device), may be automatically generated and collected.

[Reporting of unethical behavior]

Required: name and e-mail address

* Information, such as visit history during service use, job application records, records of fraudulent use, and terminal information (OS, screen size, and unique identifier of a device), may be automatically generated and collected.

[Submit Business Inquiry]

Required: Name, Affiliation(Name of Organization), Email, Contact, Inquiry Title, Inquiry Content

Optional: Website, File Attachment

* Information, such as visit history during service use, job application records, records of fraudulent use, and terminal information (OS, screen size, and unique identifier of a device), may be automatically generated and collected.

[SMTOWN website and app]

Required: name, login ID, password, email address, service usage history, access log, cookie, access IP information, terminal identification number (terminal ID), and PUSH token

*The information about the above terminal is in a form that cannot identify individuals, and the company does not engage in any activities that identify individuals based on the collected information.

[KWANGYA 119]

Required: e-mail address

*We do not collect any information other than your email address.

[Audition]

Name, date of birth, gender, country, contact information, email address, SNS account ID, information on legal representative (name, contact information, date of birth, email address) in case of applicants under 14 years of age, highest level of education, name of school that the applicant graduated from/dropped out of/attended

*Information, such as service use records during service use, access logs, cookies, access IP information, access device information, terminal identification number (terminal ID), PUSH tokens, and country of access, may be automatically generated and collected.

4. Period for processing and retaining personal information

In principle, the company retains and uses personal information for a period of time for which separate consent has been obtained from the data subject, and when the period for retaining personal information expires or the purpose of collecting and using personal information is achieved, the personal information will be destroyed immediately. However, the following information will be retained for a period of time specified for the following reasons:

〈Period for processing and retaining personal information according to relevant laws〉

- Records of marks/advertisements: 6 months (Act on the Consumer Protection in Electronic Commerce)
- Records of cancellation of a contract or order: 5 years (Act on the Consumer Protection in Electronic Commerce)
- Records of payment and supply of goods, etc.: 5 years (「Act on the Consumer Protection in Electronic Commerce」)
- Records of consumer complaints or settlement of disputes: 3 years (「Act on the Consumer Protection in Electronic Commerce」)
- Records of identity verification: 6 months (「Act on Promotion of Information and Communications Network Utilization and Information Protection」)
- Visit history (communication fact confirmation data): 3 months (「Protection of Communications Secrets Act」)

〈Processing and retention period according to company internal policy of the company〉

[Common]
In case of records of fraudulent use, personal information related to fraudulent use prevention is retained for one year from the date of collection to prevent fraudulent use.

[Recruitment]
Personal information provided during job application will be retained for 3 years from the date of collection. If consent to the processing of personal information is withdrawn or a request for withdrawal is made, however, personal information will be destroyed immediately unless there are special reasons.

[Reporting of unethical behavior]
Personal information provided when reporting unethical behavior will be retained for up to 6 months from the date of reply after the result of report processing is returned.

[Submit Business Inquiry]
Personal information provided when submitting a business inquiry will be retained for up to 6 months from the date of the reply after the submission is processed.

[SMTOWN website and app]
Personal information provided upon membership signup will be retained for up to 3 months from the date of withdrawal to improve CS response and service even after withdrawal from membership.

[Audition]
Personal information provided when applying for an audition will be retained for one year from the date of application for audition. If you request withdrawal of consent to the processing of personal information or withdrawal from membership, however, the personal information provided will be destroyed immediately unless there are special reasons.

5. Matters concerning the processing of personal information of children under the age of 14

When the company obtains consent from the legal representative regarding the processing of personal information of a child under the age of 14, it may request the child to provide the minimum information, such as the legal representative's name and contact information, and requires the legal representative to indicate whether or not he or she consents on the website where the consent is posted.

6. Matters concerning provision of personal information to third parties

The company processes the personal information of the data subject only within the scope specified in the purpose of processing personal information, and provides personal information to third parties only in cases described in Articles 17 and 18 of the Personal Information Protection Act, e.g., with the consent of the data subject or special provisions of the law. In other cases, the company does not provide the personal information of the data subject to third parties.

In the following cases, the company provides personal information to third parties only to the minimum extent necessary with the consent of the data subject in order to provide services efficiently.

[SMTOWN website and app]
Recipient: SM Brand Marketing Co., Ltd.
Purpose of providing personal information: to verify membership qualifications for the sale of member-only goods
Particulars of personal information provided: name and login ID
Retention and use period: Until withdrawal from membership

In accordance with the guidelines for handling and protecting personal information in emergency situations jointly announced by government agencies, the company may provide personal information to relevant organizations without the consent of the data subject in the event of an emergency, such as a disaster, infectious disease, an incident or accident that poses an imminent risk to life or body, or an imminent loss of property. For more information, please click here.

7. Matters concerning the entrustment of personal information processing

In order to process personal information efficiently, the company has entrusted the processing of personal information as follows:

The company manages and enforces entrustees' compliance with laws related to personal information protection, confidentiality of personal information, prohibition of provision to third parties, liability in case of accidents, period of entrustment, and obligation to return or destroy personal information after completion of processing, through entrustment contracts, etc.

The companies to which the company entrusts personal information processing are as follows:
*The entrustees may be changed depending on changes in the relevant service and the contract period, and we will notify you in advance when changing the service.

[Recruitment]
Name of the entrustee: Doodlin Co., Ltd.
Entrusted work and purpose: operation and maintenance of the talent recruitment website and storage of applicant information

[SMTOWN website and app]
Name of the entrustee: Megazone Cloud Co., Ltd.
Entrusted work and purpose: operation of the AWS service

[KWANGYA 119]
Name of the entrustee: Hyosung ITX Co., Ltd.
Entrusted work and purpose: KWANGYA 119 Report/whistleblowing operation support

[Audition]
Name of the entrustee: Picpac Co., Ltd.
Entrusted work and purpose: operation of the AWS service

8. Matters concerning overseas collection and cross-border transfer of personal information

The company provides and entrusts personal information collected from data subjects to overseas countries as follows. In principle, we back up (store) all data to recover data in the event of data loss due to a disaster or catastrophe. Therefore, if you refuse overseas transfer, you will not be able to use the service. If you do not want cross-border transfer, you can withdraw from membership on the website or request withdrawal through the customer center.

[Common]
Name of the storage company: Amazon Web Service
Purpose of storage: System Management through AWS
Particulars of personal information to be transferred: all personal information collected during the service provision process
Country to which the personal information is transferred: Japan (AWS Tokyo Region)
Date of personal information transfer: membership signup
Method of personal information transfer: storing personal information in the AWS cloud computing environment
Contact information of the entrustee: Aws-korea-blog@amazon.com

Name of the entrustee: SENDGRID
Entrusted work and purpose: Sending emails for membership signup and password resetting
Particulars of personal information to be transferred: name and e-mail address
Country to which the personal information is transferred: the US
Date of personal information transfer: membership signup
Method of personal information transfer: Transmitted over the network each time the service is used
Contact information of the entrustee: datasubjectrequests@sendgrid.com

9. Matters concerning the procedures and methods for destroying personal information

The company destroys personal information without delay when the personal information becomes unnecessary, e.g., when the period for retaining personal information expires or the processing purpose is achieved.

The procedures and methods for destroying personal information are as follows:

〈Destruction procedure〉

The information entered by the data subject for purposes such as signing up for membership is transferred to a separate database (separate file in the case of paper) after the purpose of collecting and using personal information has been achieved and is stored for a certain period of time in accordance with the company's internal policy and other relevant laws depending on information protection reasons (see the period for retaining and using personal information) and then destroyed.

〈Destruction method〉

Personal information stored in electronic files is erased using a technical method that renders the records unrecoverable. Personal information printed on paper is destroyed in a shredder or through incineration.

10. Matters concerning the rights and obligations of data subjects and legal

representatives, and how to exercise such rights

The data subject and legal representative may at any time request access, cancel processing, etc. (hereinafter referred to as "request for access, etc.") in accordance with the data subject's rights, and when the data subject requests access, etc., the company will check whether the person requesting access, etc. is the data subject or a legitimate representative. The legal representative of a child under the age of 14 may request access to, correction/erasure of, or suspension of processing of, the child's personal information.

<Request to access personal information >

Data subjects may request access to their personal information pursuant to Article 35 of the Personal Information Protection Act. However, requests to access personal information may be restricted as follows pursuant to Paragraph 5 of Article 35 of the Personal Information Protection Act.

- When access is prohibited or restricted by law
- When there is a risk of harming another person's life or body or a risk of unfairly infringing upon another person's property or other interests

< Request for correction/erasure of personal information >

Data subjects who have accessed their personal information may request correction or erasure of such information in accordance with Article 36 of the Personal Information Protection Act. However, the erasure is not permitted where other statutes or regulations stipulate that the said personal information should be collected.

<Request to suspend processing of personal information and withdrawal of consent to processing>

Data subjects may request suspension of processing or withdraw consent to processing pursuant to Article 37 of the Personal Information Protection Act. However, requests for suspension of processing may be rejected pursuant to Paragraph 2 of Article 37 of the Personal Information Protection Act as follows:

- In cases where there are special provisions in the law or it is unavoidable in order to comply with legal obligations
- When there is a risk of harming another person's life or body or a risk of unfairly infringing upon another person's property or other interests
- In cases where it is difficult to fulfill a contract, e.g., when the service agreed upon with the data subject cannot be provided without processing personal information, and the data subject has not clearly expressed his/her intention to terminate the contract.

11. Technical/administrative safeguards for personal information

In accordance with Article 29 of the Personal Information Protection Act, Article 30 of the Enforcement Decree of the Personal Information Protection Act, and the standards for ensuring the safety of personal

information notified by the Personal Information Protection Commission, the company is taking the following measures to ensure the safety of your personal information.

- Members' passwords are safely stored and managed using a one-way encryption method that cannot be decrypted.
- When transmitting and receiving personal information and authentication information of data subjects through information and communications networks, such information is encrypted through measures such as building a secure security server.
- In order to ensure the security and continuous service of the website, we are operating various programs to control network traffic and prevent attempts to illegally change information. We are making continuous managerial and technical efforts to ensure the security of the website, but please refrain from entering sensitive information that may cause problems in the event of a security breach. The company is doing its best to prevent personal information of its members from being divulged or damaged by hacking or computer viruses. In order to protect against damage to personal information, we regularly back up data, and use the latest antivirus and intrusion detection and blocking programs to prevent personal information or data of data subjects from being divulged or damaged. It also uses encrypted communication to ensure that personal information can be safely transmitted over the network.
  We are also using an intrusion prevention system to control unauthorized access from the outside and are trying to equip ourselves with all possible technical devices to ensure the security of our systems.
  - The company limits the number of employees who can process personal information to those in charge, and provides separate passwords for these individuals, which are regularly updated. In addition, the company emphasizes compliance with this privacy policy through education for those in charge. However, the company is not responsible for any problems caused by divulgence of personal information due to the data subject's own negligence or problems on the Internet.

12. Matters concerning the installation, operation and refusal of automatic personal information collection devices

The company operates "cookies" that store and retrieve information about the data subject whenever necessary. Cookies are text files that the server used to operate the company's website stores on the data subject's computer hard disk. The company uses cookies for the following purposes:

〈Purpose of using cookies, etc.〉

- We provide target marketing and personalized services by analyzing the frequency of access and visit times of members and non-members, identifying users' tastes and areas of interest, tracking their footprints, and identifying the level of participation in various events and the number of visits.
- The data subject has the option to choose whether to install cookies. Therefore, the data subject can set options in the web browser to allow all cookies, confirm whenever a cookie is stored, or refuse the storing of any cookie.

〈How to refuse cookie settings〉

- As a way to reject cookie settings, the data subject can select the options of the web browser used to allow all cookies, confirm whenever a cookie is stored, or refuse the storing of any cookie.
- How to refuse cookie settings
  -For Internet Explorer: [Tool]> [Internet option]> [personal information]> [Settings]
  -For Chrome: [Settings> [View advanced settings]> [Setting personal information contents [cookie]
- If the data subject refuses to install cookies, there may be difficulties in providing the service.

13. Additional use/provision of personal information

The company may additionally use or provide personal information without the consent of the data subject in consideration of , Paragraph 3 of Article 15 and Paragraph 4 of Article 17 of the Personal Information Protection Act and Article 14-2 of the Enforcement Decree of the Personal Information Protection Act.

The company considers the following in order to use or provide additional information without the consent of the data subject.

- Whether the purpose of using or providing additional personal information is related to the original purpose of collection
- Whether additional use or provision is foreseeable in light of the circumstances in which personal information was collected or the processing practices
- Whether additional use or provision of personal information unfairly infringes upon the interests of the data subject
- Whether necessary measures to ensure security, such as pseudonymization or encryption, have been taken

14. Privacy officer and personal information protection officer

The company is responsible for the overall management of personal information processing and has designated a privacy officer as follows to handle the complaints of data subjects and provide remedies for damages related to personal information processing. Data subjects may report, to the privacy officer, any complaints related to personal information protection that occur while using the company's services.

〈Privacy officer〉

Name: Seon Jongin
Position: Director (Technical Information Committee)
Phone: 02-6240-9800

E-mail: privacy@smtown.com

15. Processing of personal location information

The company safely manages the personal location information of data subjects in accordance with the 「Act on the Protection and Use of Location Information」 in relation to the location-based service "PASSPORT" provided by the SMTOWN app.

<Purpose of processing personal location information and retention period>

The company destroys personal location information collected in relation to the "PASSPORT" service without delay after one-time or temporary use.

<Basis for holding data confirming collection, use, and provision of personal location information, and retention period>

The company automatically records and retains confirmation data on the use and provision of personal location information of data subjects based on Paragraph 2 of Article 16 of the Act on the Protection and Use of Location Information, and stores such data for 6 months.

< Procedure for destroying personal location information and method>

After the purpose of processing personal location information has been achieved, the company safely destroys personal location information in a way that makes it impossible to reproduce it.
Personal information stored in electronic file formats is erased using a technical method that renders the records unrecoverable.
Personal information printed on paper is destroyed in a shredder or through incineration.

<Matters concerning provision and notification of personal location information to third parties>

The company does not provide personal location information to third parties without the consent of the data subject, and when providing personal location information to a third party, the company notifies the user of the recipient and purpose of provision in advance and obtains his or her consent.

<Rights and obligations of guardians of children under the age of 8 and how to exercise such rights>

In the event that the person who fall under the provisions of Paragraph 2 of Article 26 of the Act on the Protection and Use of Location Information (hereinafter the "legal guardian") of the data subjects corresponding to the following cases (hereinafter "children under the age of 8, etc.") consents to the collection, use or provision of personal location information for the purpose of protecting the life or body of children under the age of 8, etc., the company deems that such data subjects consented to it.

- Children under the age of 8
- Adult ward
- A person with a mental disability as defined in Subparagraph 2 of Paragraph 2 of Article 2 of the 「Act on Welfare of Persons with Disabilities」 and a person with a severe disability as defined in Subparagraph 2 of Article 2 of the 「Act on the Employment Promotion and Vocational

Rehabilitation of Persons with Disabilities」(limited to a person registered as a disabled person as defined in Article 29 of the 「Act on Welfare of Persons with Disabilities」)

A guardian who wishes to consent to the use or provision of personal location information for the protection of life or body of a child under the age of 8 must submit a written consent form to the company along with a document proving that he or she is the guardian.
If a guardian consents to the use or provision of personal location information of a child under the age of 8, he or she may exercise all the rights of the data subject.

<Matters concerning the personal location information protection officer>

The company's privacy officer concurrently serves as the personal location information protection officer.

16. Remedies for infringement of users' rights

Data subjects may apply for dispute resolution or consultation to the Personal Information Dispute Mediation Committee, the Privacy call center of Korea Internet & Security Agency, etc. to seek relief for personal information infringement. If you need to report or consult about other personal information infringements, please contact the following organizations.

- Personal Information Dispute Mediation Committee (http://www.kopico.go.kr,1833-6972)
- Privacy call center (http://privacy.kisa.or.kr,118)
- Information Protection Mark Certification Committee (www.eprivacy.or.kr,02-550-9500)
- Cyber Bureau of the National Police Agency (https://ecrm.police.go.kr/minwon/main,182)

17. Matters concerning changes to the privacy policy

If the company revises the contents of this privacy policy, e.g., addition, erasure or modification, in accordance with the government or company's policy, it will notify it through the home screen of the website at least 7 days in advance. If the contents of the privacy policy are changed in a way that is disadvantageous to the data subject, however, it will notify the user at least 30 days in advance so that the data subject can easily understand the contents before and after the revision.

This privacy policy will go into effect on March 28, 2025.

- Announcement date: March 21, 2025
- Effective date: March 28, 2025

You can check our previous privacy policies below.

- March 30, 2018 ~ April 25, 2019
- April 26, 2019 ~ October 17, 2023

- October 18, 2023 ~ December 31, 2024
- January 1, 2025 ~ February 27, 2025
- February 28, 2025 ~ March 27, 2025