Personal Data Processing Policy

[Effective at July 26, 2023(last update) ~ present]

We at SK Telecom believe personal data protection is crucial for its business and thus, is strongly committed to protecting privacy and confidentiality of customers' personal data. Fully complying with all the applicable laws on data privacy including the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. and the Personal Information Protection Act of Korea, we have the "Personal Data Processing Policy(the Policy)" in place and disclose it at our website(privacy.sktelecom.com) to make it readily available to any customers interested in our data privacy policy.

The Data Privacy Policy is structured as follows:

1. General principles

2. Purpose of collection and usage, scope and holding period

3. How we collect data and obtain consent

4. Outsourcing of data processing

5. Transfer to third parties

6. Data holding and usage period

7. Data deletion procedure and methods

8. Customer rights, obligations and how to exercise them

9. Personal data protection for the underage and rights of their legal guardians

10. Automatic data collection: deployment, operation, and option to refuse

11. Technical and administrative measures for data protection

12. Delivering information for advertisement purpose

13. Customer inputs and complaints

14. Personal data transfer to abroad

15. Data Privacy Manager and Office

1. General principles

• In this Policy, "personal data" refers to any information that relates to an identifiable or identified living individual, leading to the identification of that particular person. Information that falls within

any of the following categories is defined as "personal data.

1) A name or an identification card number that enables the identification of a particular individual

2) Pieces of information that may not be identifiable on their own but may lead to the identification of a particular individual when collected and pieced together

3) Pseudonymized information of 1) or 2) ('masked data') which can lead to re-identification by using or adding additional information

• We disclose our Data Privacy Policy at the front page of our website(privacy.sktelecom.com), making it readily available to you.

• The Policy may be revised based on amendments of applicable laws, regulations and guidelines or modifications to the internal rules on personal data management. Should there be a revision, a date when the revised Policy becomes effective is also provided to prevent a confusion between different versions.

• When there are revisions to the Policy, dates for the revision and enforcement, and details of the revision are published at our website(privacy.sktelecom.com).

2. Purpose of collection and usage, scope and holding period

• When collecting and using personal data, we divide consent into 'Required' for essential service provision and 'Optional' for customized service provision. Customers who do not choose 'Optional' can still use the essential services.

• We do not collect sensitive personal information that can lead to a significant privacy breach (e.g. information that reveals your race, ethnicity, faith, belief, hometown, legal domicile, political orientation, criminal records, health state, sexual life, and etc) but when it becomes necessary to collect and process some sensitive information for the purpose of service provision, a minimum level of the sensitive information can be collected after obtaining your consent in accordance with the applicable laws and regulations.

• We collect and use personal data for the following purposes:

[Purpose of collection and usage, the scope, and the holding period (Required)]

※ This includes revised or updated data in addition to the original data entered upon membership subscription.

[Purpose of collection and usage, the scope, and the holding period (Optional)]

※ This includes revised or updated data in addition to the original data entered upon membership subscription.

• We collect your personal data when you subscribe to our service through our app by accessing the saved data or the installed functions ('handset data') of your mobile handset (e.g. a smartphone or others) after notifying you that we are accessing your 'handset data'. Your personal data can be

collected and used only within the bounds of your consent.

• We can collect and use personal data required for service fee charging (i.e. a fee statement, paid/unpaid charges, total unpaid fees, etc) or automatically collected (i.e. log data, billing information, payment records, and others automatically generated in the process of executing a service contract) without your consent in accordance with the applicable laws and regulations, for purposes described in the 'Required' section. If you have given consent to the 'Optional' section, the data can be used for the purposes described in the 'Optional' section.

• We utilize video information uploaded by users to provide the JUMP AR app services, and leverage True Depth API technology for AR effects such as placing virtual items on the screen to decorate faces when filming with a phone camera. Data collected for True Depth API is not shared with or transferred to a third party.

• We may use personal data without your consent if the purpose of using the data is reasonably connected to the purpose of collecting the data as required by the applicable laws and regulations. Whether the reasonable connection is justified is determined by looking into a range of factors such as relation to the original purpose of collection, predictability based on the circumstance or practice of collecting and processing the data, a possible breach of your interest in an unjustifiable manner, or security measures taken such as data anonymization or encryption.

• We may process the collected data for statistics, scientific research, or archiving for public interest after data de-identification. Regarding the processing, outsourcing and providing the de-identified data to the third party, please see the following section. To prevent re-identification, the de-identified data is saved and managed separately and subject to necessary technical/administrative measures for data protection.

[Processing, outsourcing, and handling the third-party provision of de-identified data]

• We may generate to use or provide de-identified data(i.e. statistics, etc.) without your consent when the data no longer identifies a certain individual even when combined with other information, reasonably considering time, cost, and technology, etc. in accordance with Article 58-2 of the Personal Information Protection Act.

• We receive, collect and use the following data from other entities to provide basic services.

[Information received from other entities for basic service provision]

3. How we collect data and obtain consent

• We have a process in place to obtain your consent to 'collecting and using personal data'. You can check or click a box that says either 'I agree" or "I do not agree". When you check the 'I agree' box or click the button, we deem it as your consent to personal data collection and usage.

• You reserve the right not to allow your personal data to be collected and used, and are not subject to any forms of disadvantage. However, once you decline to give consent for services where consent is required, services we can provide to you would be limited.

• We collect personal data by obtaining your consent in various ways: We can get your signature on the written forms such as [information provided by other companies for basic service provision] in the service subscription form or an agreement on changing a username, or get consent via SKT website, app and bulletin board for customer consultation, or phone/fax when we confirm your or your agent's identity, or from our lottery events, affiliated companies, our data-collection tools for the mobile/landline/wireless internet services, or an authorized identity check agency who confirms your identity via the mobile phone verification service.

4. Outsourcing of data processing

In the service outsourcing agreement, we state the principle for our contractors that personal data should not be processed other than to deliver the contracted services, in addition to technical/administrative measures for data privacy, the objective and scope of the contracted services, limits to sub-subcontracting, other security measures such as limiting the access to personal data, our control measures such as reviewing their data privacy status, their liabilities in the event of a data breach and obligations to return or delete personal data after data processing, and we oversee compliance of our subcontractors with the agreement.

We contract out personal data processing to external specialized agencies to provide better services and more benefits to customers. The list of our subcontractors is subject to change when the service or its contract period changes. When such change takes place, it is notified through a channel decided for each service, and if there is no specific mode of notification decided, it is announced in our Notice section.

[Outsourcing of personal data processing]

5. Transfer to third parties

We use your personal data within the bounds agreed by you or allowed by the applicable laws, and we do not go beyond the agreed bounds to use or provide the data to the third-party. However, we can provide personal data without your consent if the purpose of providing it is reasonably connected to the original purpose of the collection in accordance with the applicable laws. If a situation necessitates such a decision, we make sure to consider various factors such as 'whether the decision is related to the original purpose of data collection or is predictable based on the circumstance of collection or current data processing practices, whether it infringes on your interest without any justifiable reason, or whether a security measure such as anonymization or encryption has been taken for data privacy'.

Especially in the cases described below, we can provide your personal data after taking necessary caution within the bounds described above.

A. Affiliate

We can provide for or share your personal data with our affiliates to improve our services. In the

event of providing or sharing the personal data, we shall inform you in advance via mail or e-mail about the affiliate to share data with, how much data to be shared, why we provide or share the data, and how long and how the data is managed and protected to obtain your consent. Should you decline to give consent, we do not provide or share the data with the affiliate. We will also notify to you or obtain your consent through the same process when our relationship with an affiliate changes or is terminated.

B. Divestiture, M&A, etc.

In the event of total or partial business transfer, or merger/inheritance that hands over the rights /obligations of a service provider, we notify you of such change to ensure and protect your rights regarding personal data protection.

C. When it is necessary or permissible by the applicable laws

• When it is necessary for fee payment

• When there is a special provision that allows data transfer in the applicable laws including the Protection of Communications Secrets Act, the Framework Act on National Taxes, the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Personal Information Protection Act, the Act on Real Name Financial Transactions and Confidentiality, the Credit Information Use and Protection Act, the Framework Act on Telecommunications, the Telecommunications Business Act, the Local Tax Act, the Framework Act on Customers, the Bank of Korea Act, and the Criminal Procedure Act

※ However, we do not provide your personal data just because a public agency or an investigative agency asks us to share for an administrative or investigative purpose, which is the case stipulated in 'a special provision of the applicable laws'. In such cases, we make sure to comply with the procedure required by the applicable laws such as receiving a warrant/document stamped with an official seal of the head of the organization that needs the data before providing the requested data.

We may provide your personal data as follows to enhance our service quality:

[Third-party provision of the collected personal data]

6. Data holding and usage period

We hold and use your personal data from the day your subscription starts and until the day it ends unless you have agreed to different terms and conditions or there is a legal ground that says otherwise. When you withdraw your membership or consent that has enabled personal data collection and usage, the purpose of our collection and usage of your data is achieved or terminated, or business closure or other cases deemed justifiable for service termination takes place, we destroy the collected personal data without a delay. However, if we still need to retain your personal data for service fee payment, lawsuits, conflicts, and other necessary purposes, we can retain the data until the specific purpose of retention is satisfied.

• If there is a dispute concerning product/service fees, your personal data can be retained to settle the dispute for 6 months after a contract is canceled. (However, if you have failed to pay the service fee after canceling the subscription, your personal data will be kept for 6 months after a dispute settlement, and if the payment dispute continues without being resolved, personal data will be kept until the dispute is fully settled.)

Furthermore, if there is a need to keep the membership data as dictated by applicable laws such as the Commercial Act, the Framework Act on National Taxes, the Protection of Communications Secrets Act, the Act on the Consumer Protection in the Electronic Commerce Transactions, etc, and the Credit Information Use and Protection Act, we keep the membership data for a period specified by the applicable laws. In such cases, we use the data only for the purpose of keeping the data. Examples of the reasons for, and the scope and period of holding the data are as follows according to each applicable law:

• A name, an ID number and a mobile phone number: Kept for 12 months according to the Protection of Communications Secrets Act as they need to be submitted when a service provider is requested to provide communications records of a specific member

• The date and hour of communications, the starting and ending time of communications, the assigned phone number, the number of times the service being used, and the location data of an ICT device connected to the communications network of a member whose data the service provider is obligated to have: Kept for 12 months according to the Protection of Communications Secrets Act

• A name, an ID number, the (canceled) mobile phone number, a billing address, a service charge, a service contract and any other data concerning transaction details: Kept for 5 years (personal data from a service contract that was expired or canceled more than 6 months ago is kept in a separate storage) according to the Framework Act on National Taxes, the Corporate Tax Act, the Value-Added Tax Act

• Account books, and important business documents and statements: Important documents for 10 years, and statements for 5 years according to the Commercial Act

• Log data, IP addresses and others that confirm communications history: Kept for 3 months according to the Protection of Communications Secrets Act)

• Records about displaying information for e-commerce and ads: 6 months according to the Act on the Consumer Protection in the Electronic Commerce Transactions, etc.

• Records about cancellation of a contract or a subscription: 5 years according to the Act on the Consumer Protection in the Electronic Commerce Transactions, etc.

• Records about payment and provision of goods and services: 5 years as dictated by the Act on the Consumer Protection in the Electronic Commerce Transactions, etc.

• Records about consumer complaints or dispute settlement: 3 years according to the Act on the Consumer Protection in the Electronic Commerce Transactions, etc.)

• Records about collection, processing and using credit information: 3 years as stated in the Credit Information Use and Protection Act

7. Data deletion procedure and methods

We destroy data without a delay after achieving the purpose of data collection, or when the stated holding or usage period is over. The procedure, method and timeline for the data deletion is as follows:

A. Procedure and timeline

Your personal data submitted upon service subscription is deleted or destroyed when you withdraw your subscription after being kept for a period specified in the service policy and the applicable laws. The stated period to use and keep the data can differ depending on the reasons for data protection. (See the holding/usage periods).

Even after you delete our app from your mobile handset (smartphone, etc.), your personal data may remain in our service database if you did not make a request to withdraw your consent(membership withdrawal). This means you must withdraw your consent (or membership) first if you want us to destroy all your personal data.

B. Methods to destroy data

Written documents(e.g. a subscription form) or printouts that contain personal data are shredded, incinerated or destroyed by using chemical agents. Personal data in digital forms is deleted by using technology that disables any replay or recovery of the data.

C. Separate saving and destruction of personal data of a member whose account remained dormant for a certain period

If you have not used our service for a defined period, we put your personal data in separate storage or destroy it in accordance with the following procedure unless other laws and regulations or your request says otherwise.

• No service access log for 1 year

We notify you that your personal data will be kept separately or destroyed at least 30 days before the scheduled action by using the contact number collected by our service database. However, if your contact number has not been collected by the service database, a disclosure of this personal data policy is deemed to substitute a notification.

If you are using cash points, telecom billing services, paid services, or points/miles accrued from using our service, your personal data may not be separately stored or destroyed even if you haven't used our service for longer than 1 year unless you express your will not to use our service anymore by cancelling the specific service. This is to protect your rights as our customer.

8. Customer rights, obligations and how to exercise them

A. Customer rights regarding personal data protection

You can view or be provided with information about your personal data status, records of us using or providing your data to the third party, and your consent status to our personal data policy. We have an obligation to faithfully accommodate your request to view, receive or correct your personal data, and correct or delete your personal data without a delay when correction or deletion is deemed necessary such as finding an error to personal data or personal data being kept after the mandatory holding period is over.

You can withdraw your consent to collecting/using/providing your personal data (upon subscription/cancellation). We take necessary measures to accommodate such demands without a delay. You can withdraw your consent anytime you want. However, when you withdraw your consent needed to provide essential services(i.e. membership subscription and basic service usage), we have no choice but to terminate your membership and service subscription, and you may no longer use our services.

B. Exercising your rights

You can exercise your rights described above by choosing one of the following methods based on the subscribed service. Using some of the methods may be restricted depending on the subscribed service type, the personal data type, or the level of necessity to protect personal data, and we can ask to see your ID document (an ID card, a passport, a driver's license(a new version)) and other documents that prove ownership or rights(a power of attorney, a certificate of your or your agent's seal impression).

• You can make a visit or a call to our subcontracted offices, licensed stores, or a customer center

• Click menus like 'Change Member Info' or 'Check Info' in the service section of the website, or make an inquiry to the uploaded contact number via a written form, a phone, or an email.

For mobile phone/ Internet/ phone(VoIP)/ T world services, view your personal data status by clicking 'View Personal Data Usage History' in our privacy center(privacy.sktelecom.com).

When we have a legitimate reason to refuse your request to view, prove or correct parts or all of the personal data, we notify you of the decision and provide the explanation.

C. Your obligation regarding personal data protection

For a customer's part, you should also be committed to preventing an unfortunate event by providing accurate and updated information. You are held accountable for any accident caused by inaccurate information you have submitted, and if you have submitted false or stolen information for our membership subscription, you will forfeit your membership and may be subject to punitive measures in accordance with the service agreement.

You should protect your personal data including your log-in data(ID, PW, etc.) by making sure to log out when using a shared PC. Avoid a password that is too easy or simple, and change it on a regular basis.

You should also take caution not to breach or damage the uploaded contents and other people's personal data or rights. Customers who breach or damage personal data or rights of others by violating the applicable laws will be held legally accountable.

9. Personal data protection for the underage and rights of their legal guardians

When collecting/using/providing the personal data of an underage user aged under 14 years old('an underage user'), we make sure to obtain consent of his/her legal guardian.

We may require a minimum level of information about a legal guardian such as his/her name or contact number to obtain consent of the legal guardian when an underage consumer tries to subscribe to our service. In this case, we explain to the underage consumer why we need information about his/her legal guardian and why we collect, use or provide personal data of our users in plain terms to help understanding of the underage consumer.

A legal guardian's personal data is used only for the purpose of confirming consent. We do not use or provide to the third party a legal guardian's personal data for purposes other than obtaining consent.

A legal guardian of an underage user can withdraw his/her consent, and require access to the records of personal data used by us or provided to the third parties as well as the consent status on data collection, usage and provision. A legal guardian can also request for correction when an error or wrong information is found.

10. Automatic data collection: deployment, operation, and option to refuse

We can install and operate cookies to save or view your personal information('cookies') in order to remember your preferences through services provided to you or to offer the services more efficiently. We can read the cookies in your browser when you access our services, and find additional information to enable services without asking you to re-enter your name and other personal information.

We can use your data gathered through cookies for the following purposes:

- To offer information tailored to your preferences
- To track the contents you were interested in and offer customized services at your next log-in.
- To inform you about the subscription period when you subscribe to a paid service
- To analyze your usage patterns and upgrade services based on them

You can choose to install cookies based on the way of service provision or not. For example, you can choose to accept all cookies, ask for a notice when cookies are installed, or refuse all cookies in the Tool > Internet Option > Personal Info > Advanced in the upper part of the web browser.

11. Technical and administrative measures for data protection

A. Technical measures

We have introduced following technical measures for data privacy that prevent any loss, theft, leak, falsification, or damage when we process your personal data.

• Your personal data is protected with a passcode, and critical data is protected with a separate layer of security which encrypts files and transferred data, or uses the file locking function.

• We have installed the antivirus programs on all ICT devices used for personal data processing to prevent any damage by computer viruses. Our antivirus programs are updated on a regular basis to provide the latest version, enabling a prompt response to an attack by a new virus.

• We have a security measure in place to safely transfer personal data over the network by using encryption algorithms.

• To be prepared against external attacks such as cyber hacking, we are running the anti-hacking system and the detection system that protect the internal networks in addition to deploying the access control system at each server to tighten security.

B. Administrative measures

• To maintain rigorous data privacy, we have received a third-party accreditation for our major systems and facilities such as the accreditation of the information security management system issued by a specialized outside entity.

• We have in place a rigorous procedure for personal information access and management, and make sure our employees fully understand and comply with the procedure.

• We minimize the number of employees placed to process your personal data. Those with the access and authority to process your personal data are as follows:

- Employees who interact with you and other customers directly and indirectly for marketing activities

- Employees assigned to personal data management and protection such as Personal Data Privacy Manager and Personal Data Privacy Officer

- Other employees who have no choice but to process personal data to carry out their assigned tasks

• When processing your personal data through a computer, we assign an owner who is allowed access to your personal data, give him/her an ID and a passcode to control the access and update the passcode on a periodic basis.

• We provide employees in charge of personal data processing with internal trainings and send them out for outside trainings as well about new security technologies and obligations for data security on a regular basis.

• When hiring new employees, we have them sign a data privacy pledge and a personal data privacy

pledge to put employees on alert and prevent them from breaching our Policy. We have introduced action plans for the Policy and an internal compliance monitoring procedure for sustained implementation and compliance by employees.

• When our employees leave us, we have them sign a confidentiality agreement to prevent them from damaging or breaching the personal data that have come to their knowledge during their work process.

• When employees in charge of personal data processing hand over their works to their successors, they must go through very rigorous security measures, and we have clearly defined the employee accountability when a breach happens before they join us or after they leave us.

• We have designated the data processing room, the data archive room, and other data rooms as special security areas where access is tightly controlled.

• We take necessary measures to confirm your identity when we collect or provide payment-related information such as a credit card number and a bank account number for a service subscription or provision.

• In other cases where personal information is lost, leaked, forged, falsified, or damaged, we notify you of the fact immediately and come up with appropriate measures and compensation.

12. Information for advertisement purposes

We do not send or transfer information for an advertisement purpose to make profit without your prior consent.

We obtain your consent to ads or information for commercial purposes in advance when we plan to offer you such information to carry out customer-oriented marketing by sending information on the newest products and customer events, and take various measures to make it easily recognizable that we are sending you ads.

• E-mail: We place '(ads)' or '(ads for adults)' in Korean at the first part of the mail title without a blank followed by the key message of the main content. Even when it is hard to show in the title that the message is for advertisement (e.g. via electronic devices), we take necessary measures to show the sender's name to inform you that it is advertisement information.

• Fax, SMS and other methods: We take necessary measures such as showing the sender's name.

When you give consent, refusal, or withdrawal to receiving ads information, we will notify you of the fact in less than 14 days for confirmation. We also confirm with you about your status on receiving ads or information for commercial purposes every 2 years from the date you give us the consent.

13. Customer inputs & complaints

We value your opinions. Should you have any inquiries, please contact our customer center for accurate information in prompt response. The contact information of our customer center is as follows:

- Phone : 1599-0011

- Online customer center:

. Log on to www.tworld.co.kr and find VoC/Info under the Customer Center menu to leave your inquiry.

. Log in to the app market such as Google Play or One Store, etc. to give an inquiry to a service developer.

For detailed contact information to leave VoC on individual services, please see 'Attachment 6. Customer inputs and complaints')

[Customer inputs and complaints]

14. Overseas data transfer

If necessary, we can subcontract or place your personal data overseas. The scope of personal data that can be outsourced for processing or kept overseas is as follows:

[Privacy data transfer to overseas]

15. Data Privacy Manager and Officer

We are doing our utmost to protect your personal information and make sure you use our services safely. We have designated Personal Data Privacy Managers and Officer as below to take care of related inquiries, complaints, and remedies against damage, and provide prompt and kind responses to your request.

Data Privacy Manager: skt.privacy@sk.com

[See the full list of Data Privacy Officer/Managers]
[Location Information Manager and Responsible Department]

- Announced at July 26, 2023
- Came into force at July 26, 2023