



Korea's PIPA



Disclaimer

A word from our lawyers: Nothing stated here is legal advice. It is provided for your information and convenience. We strongly encourage that you work closely with legal and other professional advisors to determine exactly how the Korea's Personal Information Protection Act applies to you.

What is the PIPA?

In Korea, privacy and data protection is regulated by the Personal Information Protection Act of 2011 ('PIPA'), which is a comprehensive, principles-based law that applies to personal information processors. PIPA applies to Korean companies as well as companies that process personal information in Korea.

What information does the PIPA apply to?

Personal information under PIPA pertains to living persons and is any data that can be used to identify an individual. Like for example the GDPR, information will also be considered personal if it can be combined with other information to identify a specific individual.

Sensitive data includes information such as an ideology, belief, membership of a trade union or political party, political mindset, health and sexual life. Sensitive data also includes any other personal information which is likely to cause harm to the privacy of a data subject.

PIPA distinguishes data controllers and data processors. Under PIPA, a controller is called a "Personal Information Manager" and the processor is the "Data Consignee."

PIPA compliance in respect of using AppsFlyer

AppsFlyer restricts customers from configuring the service to collect personal data such as names, contact information, addresses, financial information or any sensitive personal data. However, due to the very broad definition of "Personal Information" under PIPA, it is likely that device identifiers such as Advertising ID's (IDFA, GAID) or network data such as IP address will be deemed personal information and thus the information collected when using AppsFlyer will be subject to the PIPA requirements.

Under PIPA, personal information can be collected and shared with a third party if one of the following conditions has been satisfied:

- consent has been provided by a data subject;
- it is required by law;
- it is required for the processor to carry out work under laws and regulations;
- it is necessary to execute and perform a contract with the data subject;
- necessary for the protection of the data subject or a third party, such as a legal representative, from danger to life, body or economic profits.

When transferring personal information to third parties, processors must inform the data subject of the recipient, purpose for sharing, type of personal information shared, period of use.

Direct marketing data subjects must be notified if personal data will be used to promote or sell goods or services.

What rights do individuals have under the PIPA?

Under PIPA, data subjects have the right to:

- Be informed of their rights and how the information will be used;
- Request access to their personal information;
- Request correction to their personal information; and
- Request erasure of their personal information.

For such deletions, AppsFlyer has implemented the Open DSR API.

Can customers opt out an end user from measurement if they don't provide consent?

Yes, AppsFlyer provides its customers with multiple options to support whatever framework customers wish to implement. These include the opportunities for end users to opt-in or opt-out of such measurement, or the customer can determine that it does not wish to share data with potential partners. AppsFlyer's service is highly configurable to allow compliance with PIPA and other local data protection laws.

Does PIPA restrict international transfers of personal information?

No. However, for the purposes of transferring personal information across borders, explicit consent must be obtained from the data subject and the data must be protected in accordance with the standards of PIPA.

What are the consequences for non-compliance?

Non-compliance with PIPA has various consequences. These include fines of up to 100 Million won (KRW) and imprisonment of up to 10 years may be issued as punishment for breaches of PIPA.