



Japanese Act on Protection of Personal Information & Telecommunications Business Act



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 Japanese Act on Protection of Personal Information and the Telecommunications Business Act apply to you.

What are the APPI and the TBA?

The APPI (Act on Protection of Personal Information) is Japan's privacy regulation that came into effect on April 1, 2022. The TBA is Japan's Telecommunications Business Act which came into effect in June 2023.

Scope of Application of the APPI and TBA

Similar to the GDPR, the APPI has an extra-territorial scope. It therefore, also applies to those in a foreign country handling any personal information (including pseudonymized and anonymized) that relates to data subjects in Japan, when this is in relation to the supply of goods or services in Japan. These entities processing data are called personal information handling business operators ('PIHBO's).

The APPI defines personal information broadly, including:

- a name, date of birth or other description,
- a drawing or electromagnetic record,
- scenarios where the information can be connected with other information data used to identify a specific individual;
- data containing an individual identification code.

Along with Personal Information, the APPI regulates 'Personally Referable Information' ('PRI'): information which is related to personal matters, but that does not fall under the definition of Personal Information. PRI includes, among other things, a web browsing history collected through the terminal identifier such as cookie information, a person's age, gender or family makeup that are linked to his / her email address, a person's purchase history of goods and / or services, a person's location data, or a person's area of interest. The handling of PRI is not regulated as Personal Information, but prior consent from data subjects would be required to transfer PRI in certain circumstances.

The APPI also defines 'sensitive information', which includes personal information such as an individual's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions.

The TBA is more narrow in scope and applies to telecom businesses providing services such as communications, social media services, live streaming and gaming, or news sites and search engines.

Under what terms are AppsFlyer's customers allowed to collect and process Personal Information under the APPI and the TBA?

PIHBOs must not obtain personal information by deceit or improper means. In order to collect personal information, PIHBOs must provide notice to the 'principal' (the individual whose personal information was acquired and allow for an opt-out). In AppsFlyer's situation this would be the customer's end-user. Such notice is typically provided through a privacy policy that customers may place on their website or in their app.

Personal information under the APPI must be used for a specific purpose and any new purpose would require consent unless an exception applies.

Consent is also needed for the transfer of cookies to third parties, as the APPI determines that cookies are "Personally Referable Information".

Under the TBA, first party cookies are exempt.

The TBA requires notification of collected data points that would be shared with a third party, the purpose of collection and who that third party would be. Such notification must be in plain language, in Japanese and readily available through popups or as a banner. Furthermore, similar to the APPI, consent and opt-out mechanisms are required.

Consequences for non-compliance with the APPI and TBA

- Penalties for business operators can include:
- Up to one year imprisonment or a maximum fine of ¥500,000 for disclosing personal information for the purpose of illegal profit;
- Up to one year imprisonment or a maximum fine of ¥1,000,000 for a business operator violating an order from the PPC;
- Up to six months imprisonment or a maximum fine of ¥500,000 for a business operator failing to submit or providing false reports to the PPC upon request;
- Penalties may also apply to representatives of a business operator, such as an individual employee.

Penalties under the TBA for non-compliant businesses may see similar penalties regarding false reporting or invasion of inspection.

Guide to APPI compliance in respect of using AppsFlyer:

Customers will first need to establish an APPI appropriate lawful basis to collect personal information from their end users. Some of the lawful bases covered under the APPI are similar to those under the GDPR.

However, the most appropriate lawful basis to cover a customer's use of AppsFlyer will likely be the provision of 'notice' and consent. This is due to the fact that the APPI does not have a GDPR like "legitimate interest" lawful basis. As a result, customers will need to make sure to obtain appropriate consent from their users in respect of their collection of personal information and sharing of this data in such a manner with AppsFlyer. Those customers considered a business under the TBA would also need to consider obtaining consent from their users.

AppsFlyer restricts customers from configuring the service to collect personal data such as names, contact information, addresses, financial information or any sensitive personal data, including as part of the customer's CUID. The PPC has stated that a web (or app) browsing history, collected through identifiers such as cookies, an IP address, location data, information exchanged on DMPs (data management platforms) containing identifier information, and similar technologies, all constitute PRI.

The information collected by customers when using AppsFlyer in such a manner will be subject to the APPI requirements. In order to obtain appropriate consent, customers will also need to provide their end users with proper notice of their data collection and use practices. Customers may view [AppsFlyer's Service Privacy Policy](#) to gain a broader understanding of the categories of data processed by AppsFlyer on behalf of customers.

Note that this is needed for all partners customers decide to integrate with also.

Individuals Rights under the APPI

Under the APPI, individuals have the right to:

- be informed of their rights prior to collection and use of their personal information;
- request correction, rectification and/ or deletion of their personal information held by PIHBOs;
- object to processing by lodging a utilization cease request, based on reasonable grounds; and
- lodge complaints to the PPC or any other authorized entity about the handling of their personal information.

AppsFlyer enables customers to comply with their obligations under the APPI and other privacy regulations in respect of individual rights.

Specifically, AppsFlyer provides the OpenGDPR framework to enable customers to automatically submit individual deletion and data access requests for personal data that has been transferred to AppsFlyer.

AppsFlyer is also committed to maintaining appropriate internal management systems and operating procedures as well as appropriate technical security measures to protect customer data. For more information on such measures please visit our [Trust Hub](#).

Cross-border transfers under the APPI

The APPI states that Personal information may be transferred outside of Japan where:

- consent is obtained from the principal;
- the foreign state has privacy laws which are considered equivalent to Japan; or
- the foreign party maintains an internal personal information protection system consistent with standards set by the Japanese Personal Information Protection Commission (PPC).

This means that customers must also ensure to be able to provide their end users with the appropriate information on transferring data outside of Japan to AppsFlyer when they request such information.

AppsFlyer stores all customer and end user data within the EU, which has been recognized by Japan as an equivalent level of protection to the APPI.

AppsFlyer's DPA and data processing

Customers can feel confident that AppsFlyer will continue to process personal data in accordance with the requirements of the APPI and other global laws. Besides AppsFlyer operating as an entrusted party and not using the personal data for any reason other than to provide the services requested by the customer, AppsFlyer provides a special [data protection addendum](#) to cover its processing of the personal data. This DPA covers a range of issues such as AppsFlyer's commitment to implement appropriate technical and organizational measures to protect personal data, to assist customers with their compliance needs including by cooperating in respect of data protection impact assessments, individual rights request (such as the right of deletion), breach notification requirements and more.

We also would like to emphasize that the nature of the data AppsFlyer needs to receive in order to provide the services does not include any sensitive or direct personal information under the APPI and is limited to personal data that is pseudonymised by nature e.g. advertising device IDs, IPs. Therefore, we are confident that our existing measures will be sufficient to ensure complete compliance with APPI requirements. Indeed, customers will need to also assess any additional laws applicable to them, such as the TBA, given their own products since certain unique industry specific obligations may apply to them in addition to the APPI.

Future Compliance

As a final note, since the APPI is a comprehensive law and has a broad set of obligations, it is important that every customer assess the APPI and TBA with their advisors taking into consideration the nature of their own services and take the necessary steps to ensure compliance. AppsFlyer is here to assist you in ensuring such compliance.

Be assured that AppsFlyer is continuously monitoring the developments around the APPI and TBA, its enforcement and the cross border frameworks and is working diligently to ensure that customers will be able to continue to use AppsFlyer in full compliance with the APPI and TBA and other global laws.