India's 'Digital Personal Data Protection' Act 2023

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 India's 'Digital Personal Data Protection' Act applies to you.

AppsFlyer

What is the DPDP?

In India, privacy and data protection is regulated by the 'Digital Personal Data Protection' Act of August 2023 (DPDP). This comprehensive bill applies to the processing of digital personal data, meaning data that is collected online or which is digitized after collection.
The DPDP is a 'principles-based legislation' that applies to similar concepts as can be found in the GDPR. The DPDP covers a 'data fiduciary' (controller), data processors and data principals (data subjects).
The DPDP is applicable to data processed within the Indian territory and extraterritorial processing in connection with offering of goods and services to data principals within India.

What information does the DPDP apply to?

Personal data under DPDP is any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.
Data excluded by the DPDP is aggregated data as collected for research or statistical purposes which is not used for decision making related to a 'data principal'. Publicly available data has also been excluded from the DPDP, in contrast to such data under the GDPR for example.
The DPDP does not differentiate between 'regular' personal data and sensitive personal data.

Does the DPDP restrict international transfers of personal data?

No. The DPDP allows for international, cross-border transfers to all countries except those specifically excluded and restricted by the Indian government. The DPDP's approach aligns with general international principles on data transfer.

DPDP 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, health information or any other type of particularly sensitive personal data. However, due to the very broad definition of "Personal data" as data that may identify a data principal under DPDP, 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 some of the information collected when using AppsFlyer will be subject to the DPDP requirements.

AppsFlyer would be a data processor under the DPDP and AppsFlyer's customers would be considered 'data fiduciaries' (controllers) under the DPDP.

The DPDP's main legal basis for the collection of personal data is consent, which would be an affirmative 'opt-in' consent as provided by an app user. Consent must be requested with a prior notice by the data fiduciary (controller) containing details on the data to be collected and the purpose of its processing. The DPDP recognizes a very limited set of "legitimate uses" of data processing that do not require consent, including:

- Voluntary provision of data by the individual without added objection
- Employment
- Fulfillment of legal obligations
- Medical emergencies or public order
- Governmental services

Note: the data principal has the right under the DPDP to request from the data fiduciary the identity of any data processors with whom data has been shared, along with a description of the data shared.

The DPDP and Minors

A major difference between the DPDP and other privacy legislation concerning children (such as the GDPR in the EU and COPPA in the USA), is that the DPDP considers all minors below the age of 18 as children warranting the 'verifiable' consent of a parent or legal guardian prior to the processing of personal data.

The DPDP explicitly addresses further restrictions for data fiduciaries regarding the processing of personal data of such minors:

- The processing may not be undertaken if it is likely to cause any detrimental effect on the well-being of a child;
- The processing shall not include the tracking or behavioral monitoring of children, or targeted advertising directed at children.

The Indian government maintains the right to assess circumstances in which these restrictions may be exempt for specific data fiduciaries that have been able to satisfy the government that the processing of data is verifiably safe.

When using AppsFlyer in compliance with the DPDP, it is important to ensure the implementation of apps in a manner that is in accordance with the AppsFlyer Kids Compliance Guide. This Guide details the manner in which you can implement the AppsFlyer SDK in accordance with relevant settings for the protection of children's privacy.

What rights do individuals have under DPDP?

Data principals have a number of rights under the DPDP, including a right to correction, completion, updating and erasure of their personal information, as well as the right to withdraw consent and the right of grievance redressal.

Most commonly applicable to AppsFlyer's processing of a data principal's data is the right to erasure of personal data. For such erasure, AppsFlyer has implemented the Open DSR API which allows for automated deletions.

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

Consent may be withdrawn at any point in time by data principals under the DPDP. Therefore, 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. Also, 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 DPDP and other local data protection laws.

What are the consequences for non-compliance with the DPDP?

Non-compliance with DPDP has various consequences, including fines of up to 30 million USD (two hundred and fifty crore rupees). In particular, failure to prevent a data breach by taking reasonable security safeguards will be penalized financially.