



# Thailand's PDPA



Thailand's consolidated data protection law entered into force on June 1, 2022.

At AppsFlyer, privacy and security are always at the forefront. To ensure our customers have the tools and assurances they need to comply with the PDPA, AppsFlyer has taken the following actions:

**A word from our lawyers:** Nothing stated here is legal advice. It is provided only for your informational and convenience purposes. You should work closely with legal and other professional advisors to determine exactly how the PDPA or any other laws may or may not apply to you.

## Update to its Terms and Data Protection Addendum

AppsFlyer extended its Data Protection Addendum (“DPA”) and commitments under the DPA to cover personal data as defined under global regulations including the PDPA and not only personal data subject to the GDPR. The DPA is incorporated into the AppsFlyer terms of use by reference and therefore customers will not need to take any actions. The changes will take effect immediately. The DPA is available here: <https://www.appsflyer.com/gdpr/dpa.pdf> and includes, among other things:

1. A definition of each party’s status under the PDPA: AppsFlyer as a Data Processor and Customer as the Data Controller;
2. AppsFlyer’s commitment to:
  - a. processing data per the instructions of its customers as provided under their agreements;
  - b. ensuring it has appropriate technical and organizational measures to protect customer’s personal data;
  - c. supporting customers with their compliance requirements including those related to reporting, data breaches, and data subject rights; and
3. A list of the subprocessors utilized by AppsFlyer and the procedures for adding any new subprocessors

For customers who have executed a previous version of the DPA or wish to have an executed copy of the DPA, you are welcome to download and execute the new version available at <https://www.appsflyer.com/gdpr/dpa.pdf> (which has been pre signed by AppsFlyer) and to submit an executed copy to [privacy@appsflyer.com](mailto:privacy@appsflyer.com). Regardless of whether you execute such modified version or not, be assured that AppsFlyer will process personal data subject to the PDPA pursuant to the terms set forth under the updated DPA.

## **Data Subject Requests Support**

AppsFlyer already has an infrastructure in place in support of the GDPR and CCPA, enabling customers to [make data deletion and access requests](#) through simple API calls utilizing the OpenGDPR framework.

Customers will be able to utilize OpenGDPR to comply with any data subject access and deletion requests they receive under the PDPA.

# FAQs

## What is the PDPA?

The Personal Data Protection Act 2019 is a new privacy regulation in Thailand which was published in May 2019 and comes into full effect on June 1, 2022. The PDPA derives many of its principles from the GDPR, Similar to Europe's GDPR, the intention of the PDPA is to harmonize and strengthen the protection of personal data in Thailand, empower individuals and to reshape the way organizations handling personal data approach data privacy.

## Who does the PDPA apply to?

The PDPA has an extraterritorial scope applying to companies regardless of where they are headquartered or where the personal data is actually processed.

Specifically, the PDPA will apply to you if:

- You are a data controller or data processor in Thailand; or
- You are outside of Thailand and either:
  - collect, use, and disclose data in relation to the offering of goods or services to data subjects in Thailand; or
  - collect, use, and disclose data in relation to the monitoring of data subject's behavior in Thailand

Therefore, in practice, you should assume you are subject to the PDPA, regardless of where you are headquartered if the personal data processed relates to individuals located in Thailand.

## **What information does the PDPA apply to?**

The PDPA applies to personal data which is defined broadly to cover any data that, either directly or indirectly, enables identification of a natural person.

## **Under what terms are companies allowed to collect and process Personal Data under the PDPA?**

Similar to the GDPR, the PDPA requires entities to have a legal basis in order to collect and/or process personal data. These include:

1. consent;
2. as needed for execution of a contract with a data subject;
3. to comply with a legal obligations;
4. for the protection of the life, health or physical safety of the data subject;
5. for the public interest;
6. for for preparation of historical documents or archives in the public interest or research;
7. for legitimate interests of the controller or third party

Separate lawful bases are required in order to process sensitive personal (data pertaining to racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data). These include:

1. explicit consent;
2. for the protection of the life, health or physical safety of the data subject when consent not possible;
3. foundations, associations, or non-profit bodies carrying out legitimate activities for their members or associated individuals when not disclosed outside the organization;
4. for the establishment, compliance, exercise, or defense of legal claims;
5. for other legal reasons including: preventative medicine and managing health and social care systems; public interest and health; employment protection, social and national health welfare and scientific, historical, and statistic research purposes.

Customers are contractually required not to provide sensitive personal data with AppsFlyer.

### **What rights do individuals have under the PDPA?**

With transparency as one of the PDPA's key principles, individuals have a general right to be informed of the processing in a clear, adequate and ostensive manner. Customers are required to review their privacy policies and ensure they accurately describe their privacy practices. Data subjects will also have the following rights:

- access to the personal data processed
- erasure or deidentification of personal data
- right to object or opt out of certain processing such as in relation to direct marketing
- portability of data provided by the data subject when the lawful basis is consent or to perform a contract;
- rectification;
- not to be subject to automated decision making in certain cases
- to withdraw consent

### **What rights do individuals have under the PDPA?**

Consequences may include fines and penalties that reach up to THB 5 million, and criminal penalties that can include imprisonment for up to 1 year or THB 1 million.

# What this means for customers using AppsFlyer

## Who is the Controller and Processor?

Similar to the GDPR, the PDPA separates between the data controller and the data processor.

- The **data controller** is the person or entity in charge of making decisions regarding the processing of personal data
- The **data processor** is the person or entity that processes personal data in the name of the controller

In the context of using the AppsFlyer services, the data controllers are AppsFlyer's customers and the data processor is AppsFlyer.

The AppsFlyer services are essentially an extension to the customer's technology stack (similar to a CRM). The personal data processed belongs to the customer. AppsFlyer will only process the personal data to provide the service as instructed by the customer under the terms of the agreement between the parties (and as further described in the [AppsFlyer privacy policy](#)).

As data controllers, AppsFlyer's customers will need to comply with all requirements of the PDPA that apply to them as data controllers.

Controllers will need to, among other things:

- establish a legal basis for the collection of data (e.g. consent, legitimate interests)
- provide appropriate privacy notices to data subjects about their personal data processing
- ensure they have procedures in place to respond to data subject requests



- maintain appropriate records of their data processing (data mapping)
- ensure records of valid consents maintained when legal basis is consent
- appoint a data protection officer and publish his or her contact details
- implement an appropriate data security program and incident response plan for data breaches (to ensure notice to regulator within 72 hours and without undue delay to data subjects where high risk to freedoms and rights)
- implement privacy by design principles
- comply with cross border transfer requirements

## **Is the information that customers collect through AppsFlyer considered “Personal Data” under the PDPA?**

Even though AppsFlyer restricts customers from configuring the service to collect personal data such as names, contact information, addresses, financial information or any sensitive personal data, due to the very broad definition of “Personal Data” under the PDPA, it is possible (although no final guidance has been provided on the matter) that device identifiers such as Advertising ID’s (IDFA, GAID) or network data such as IP address will be deemed personal data and thus the data collected when using AppsFlyer will be subject to the PDPA requirements.

For more information on the data types processed when using AppsFlyer please visit the [AppsFlyer Services Privacy Policy](#).

## **Can AppsFlyer support deletion or access requests?**

AppsFlyer already has an infrastructure in place in support of the GDPR and CCPA that enables customers to make data deletion and access requests through simple API calls utilizing its [OpenGDPR framework](#).

## **Can personal data be transferred and processed outside of Thailand?**

Yes, international transfers will be permitted provided there is a valid legal basis – for example, where prior valid consent was given or to perform a contract.

transfers will be permitted to a country or organization that provide an adequate level of protection of personal data as approved by the Thai Data Protection Authority (the "PDPC"), or where there are guarantees of compliance to the PDPA principles through :

- agreement of specific protection measures ;
- Global binding corporate rules;

However, the PDPC has yet to prescribe any rules in regards to specific protection measures and has yet to deem any countries adequate.

Therefore, since AppsFlyer processes personal data outside of Thailand (primarily in the EU and Israel), and even though it offers a Data Protection Addendum with specific protection measures, Customers should ensure they receive valid consent from their end users.

AppsFlyer will process personal data under the terms of its Data Protection Addendum (available [here](#)), which were initially established in respect of processing personal data subject to the GDPR and thus ensure a high standard of data protection closely aligned to the requirements of the PDPA.

### **Can data be kept only in Thailand?**

No. Currently AppsFlyer processes its data at AWS and Google Cloud in the EU. In providing support and maintenance to AppsFlyer customers, data may also be accessible in other territories where AppsFlyer provides services, including, Israel. More information about AppsFlyer's subprocessors can be found [here](#).

### **Can we 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 (opt-in, opt-out, no postbacks etc).