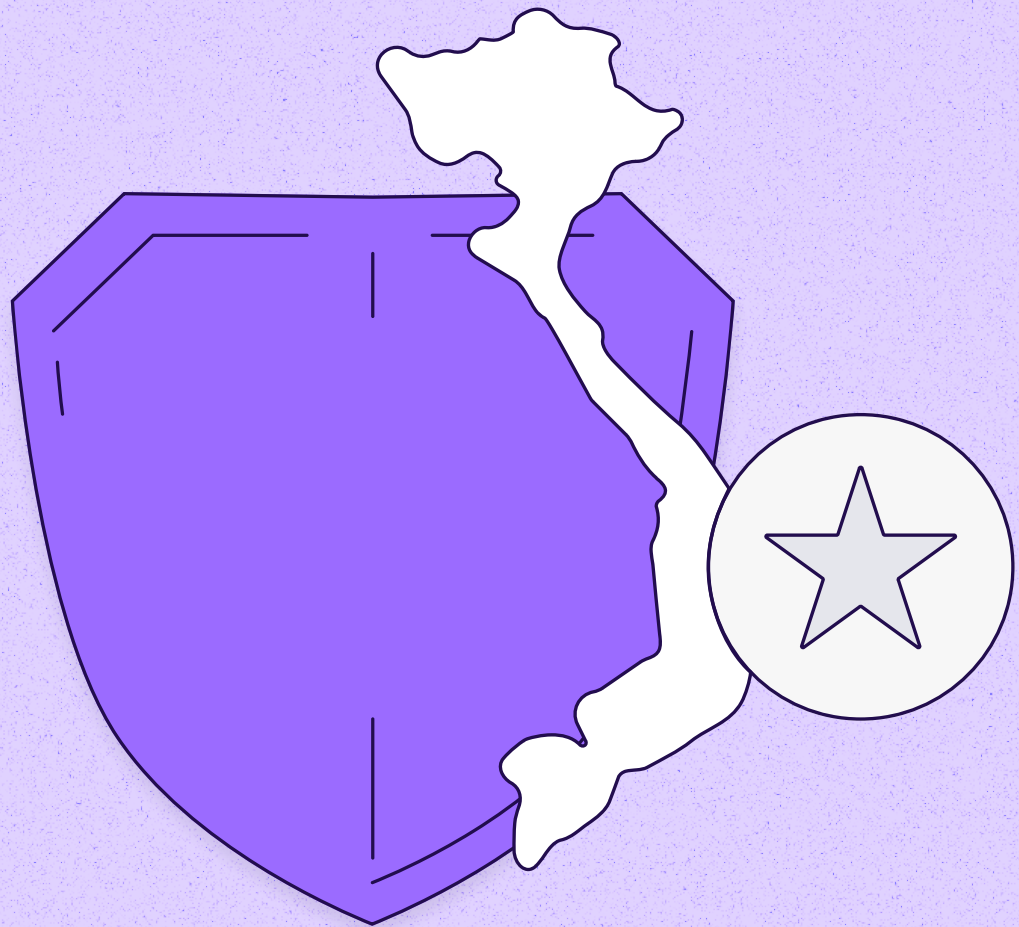


# Vietnam's Decree of Personal Data Protection



**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 Vietnamese Decree of Personal Data Protection (PDPD) applies to you.**

### **What is the PDPD and what is its scope of application?**

In Vietnam, privacy and data protection is regulated by the governmental Decree of Personal Data Protection ('PDPD'), which aims to synchronize the data protection regime in Vietnam. The law went into force in July 2023.

Similar to the GDPR, the PDPD distinguishes between entities functioning as a data 'controller' and those operating as a data 'processor', but also recognizes an entity can function both as a processor and controller.

Processing activities within the scope of the PDPD include

- Personal data processed within Vietnam
- Vietnamese entities processing personal data, regardless of whether the data is processed within the territory of Vietnam
- Foreign entities processing personal data of Vietnamese nationals

The DPDP codified multiple legal bases for the processing of personal data. Unlike the GDPR, the DPDP does not, however, recognize 'legitimate interest' as a basis for the processing of personal data, and controllers will need to rely on the bases of 'consent' or 'contractual necessity', depending on the circumstances. Such consent will need to be active, for example through the requirement of an opt-in.

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

The PDPD defines personal data as 'electronic information in the form of symbols, letters, numbers, images, sounds, or equivalences associated with an individual or used to identify an individual'. This includes name, address, date of birth, and email. Under the Decree, personal data is differentiated into general personal data and sensitive personal data. In particular, sensitive personal data refers to those parameters that, when infringed upon, will directly affect the individual's legal rights and interests. This includes, but is not limited to political or religious associations; health information; racial, ethnic, genetic or sexual life information; financial information and criminal activities.

The PDPD furthermore includes 'information used for the identification of an individual' which refers to that information which may identify an individual, if and when combined with other information or data, in a similar manner as the definitions in the GDPR.

Including AppsFlyer's customers, are affected.

## **PDPD compliance in respect of using AppsFlyer**

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

AppsFlyer customers must ensure that personal data is collected in a manner consistent with the PDPD, such as consent, performance of a contract with the data subject or legal requirement. Furthermore customers must ensure the performance of a DPIA prior to sharing data with a third party such as AppsFlyer. The sale and purchase of personal data is furthermore prohibited under the PDPD, but consent of the data subject would allow for sharing for these purposes. Clear information sharing with the data subject on the purposes of data processing is also required under the PDPD.

### **Does PDPD restrict international transfers of personal information?**

For the purposes of transferring personal information across borders, explicit consent must be obtained by customers from the data subject and the data must be protected in accordance with the standards of PDPD that include a DPIA.

A copy of data may be shared externally, if local storage is also provided in accordance with Decree 53 that applies together with the PDPD. For this purpose, AppsFlyer works with local AWS servers within Vietnam.

### **What rights do individuals have under PDPD and how does AppsFlyer enable compliance?**

Under PDPD, data subjects have several data protection rights, including the right to:

- know how their information will be processed;
- request access to their personal information;
- request correction to their personal information;
- restrict or object to their data being processed; and
- request erasure of their personal information.

AppsFlyer has implemented the [Open DSR API](#) for the purpose of allowing customers' end users to make requests for deletion from our services.

[Opting out](#) of measurement and other privacy preserving controls (such as opt-in) are also available to customers. AppsFlyer provides its customers with multiple options to support whatever framework customers wish to implement. A customer can also determine whether it does or does not wish to share data with ecosystem partners. AppsFlyer's service is highly configurable to allow compliance with the PDPD and other local data protection laws.